System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

GCM 8000 Comparator

NOVEMBER 2016

MN003277A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003277A01-A	Original release of *GCM 8000 Comparator* manual	November 2016
MN003277A01-B	Updated Initial Configuration of a Device in CSS on page 73	November 2016

This page intentionally left blank.

Contents

Copyrights **3**
Contact Us **5**
Document History **7**
List of Figures **15**
List of Tables **17**
List of Processes **19**
List of Procedures **21**
About GCM 8000 Comparator **23**
What Is Covered In This Manual? 23
Helpful Background Information 23
Related Information 24
Chapter 1: GCM 8000 Comparator Description **25**
1.1 What Is the GCM 8000 Comparator? 25
1.2 Supported System Configurations 26
1.3 GCM 8000 Comparator Functions 26
1.3.1 Simulcast Function 27
1.3.2 Voting Function 27
1.3.3 Multicast Function 28
1.3.4 Data Steering 28
1.3.5 Console Interface 28
1.3.5.1 MCC 7500 AUX I/O Server 28
1.3.5.2 MCC 7500 Console 29
1.3.6 Redundancy Function 29
1.3.7 License Auditing 30
1.4 Subsite Topology 30
1.5 How Does a GCM 8000 Comparator Work? 30
1.6 Specifications 31
Chapter 2: GCM 8000 Comparator Theory of Operation **33**
2.1 GCM 8000 Comparator 33
2.2 Fan Module 33
2.3 Power Supply 34
2.3.1 AC/DC Power Distribution 35
2.3.2 Power Supply Battery Charger 35
2.3.3 Battery Temperature Sensor Cable 36
2.3.4 ON/OFF Switch for Power Supply and Battery Charger 36

2.3.5 Power Supply Module Backplane Connections..... 36
2.4 Auxiliary Power..... 37
2.5 Network Fault Management..... 37
Chapter 3: GCM 8000 Comparator Installation..... 39
3.1 Pre-Installation Tasks..... 39
3.1.1 Equipment Installation Process Overview..... 39
3.2 General Safety Precautions..... 40
3.2.1 DC Mains Grounding Connections..... 41
3.2.1.1 Disconnect Device Permanently Connected..... 42
3.2.1.2 Multiple Power Source..... 42
3.2.1.3 Connection to Primary Power..... 42
3.2.1.4 Replaceable Batteries..... 42
3.2.2 Maintenance Requiring Two People..... 42
3.2.3 Equipment Racks..... 42
3.3 General Installation Standards and Guidelines..... 42
3.3.1 General Site Preparation Overview..... 43
3.3.2 General Equipment Inspection and Inventory Recommendations..... 44
3.3.3 General Placement and Spacing Recommendations..... 44
3.3.4 General Cabinet Bracing Recommendations..... 44
3.3.5 Mounting Cabinets or Racks to a Floor..... 45
3.3.6 General Bonding and Grounding Requirements..... 45
3.3.7 General Cabling Requirements..... 45
3.3.8 General Power Guidelines and Requirements..... 46
3.3.8.1 General AC Power Guidelines and Requirements..... 46
3.3.8.2 General Breaker Recommendations..... 47
3.3.8.3 General Battery Installation Recommendations..... 47
3.3.9 General Electrostatic Discharge Recommendations..... 47
3.3.10 FCC Requirements..... 48
3.3.11 Networking Tools..... 48
3.3.12 General Installation/Troubleshooting Tools..... 48
3.3.12.1 General Tools..... 48
3.3.12.2 Rack Tools..... 49
3.3.13 Technical Support for Installation..... 50
3.3.13.1 Site-Specific Information..... 50
3.4 GCM 8000 Comparator Hardware Installation..... 50
3.4.1 Placement and Spacing..... 51
3.4.2 Power Requirements..... 51
3.4.3 GCM 8000 Comparator Mounted in a Rack..... 52
3.4.3.1 Mounting the GCM 8000 Comparator..... 53

3.4.4 Grounding..... 53
3.4.4.1 Bonding and Grounding General Requirements..... 53
3.4.5 Battery Temperature Sensor Mounting..... 54
3.4.6 GCM 8000 Comparator Front Ports..... 57
3.4.7 GCM 8000 Comparator Rear Ports..... 58
3.5 Installing Device Software Prerequisites..... 59
3.6 Software Download Manager..... 61
3.7 Installing Devices in the UNC..... 62
3.7.1 Discovering a Device in the UNC..... 63
3.7.2 Loading Device OS Images to the UNC..... 64
3.7.3 Loading Software to a Device..... 65
3.7.3.1 Enabling FTP Service..... 65
3.7.3.2 Transferring and Installing the OS Image..... 66
3.7.3.3 Inspecting Device Properties for Transferred and Installed Software..... 68
3.7.3.4 Disabling FTP Service..... 69
Chapter 4: GCM 8000 Comparator Configuration..... 71
4.1 Configuration Software..... 71
4.2 Discovering a Device in the UNC..... 71
4.3 Default Speed/Duplex Settings..... 72
4.4 Security/Authentication Services..... 72
4.5 Device Configuration in CSS..... 73
4.5.1 Initial Configuration of a Device in CSS..... 73
4.5.2 Connecting Through a Serial Port Link..... 74
4.5.3 Serial Connection Configurations..... 75
4.5.3.1 Setting the Device IP Address and Pairing Number in CSS..... 75
4.5.3.2 Pairing To a Base Radio/Receiver..... 76
4.5.3.3 Serial Security Services in CSS..... 77
4.5.3.4 Resetting SNMPv3 User Credentials to Factory Defaults in CSS..... 78
4.5.4 Connecting Through an Ethernet Port Link..... 78
4.5.5 Ethernet Connection Configurations..... 81
4.5.5.1 Setting the BR/CM Pairing Number in CSS..... 81
4.5.5.2 Setting the Date and Time in CSS..... 82
4.5.5.3 Changing SNMPv3 Configuration and User Credentials in CSS..... 82
4.5.5.4 Customizing the Login Banner in CSS..... 85
4.5.5.5 Setting the SWDL Transfer Mode in CSS..... 86
4.5.5.6 Setting the Local Password Configuration in CSS..... 87
4.5.6 CSS Configuration Parameters for a Trunked GCM 8000 Comparator..... 88
4.5.7 CSS Configuration Parameters for a Conventional GCM 8000 Comparator..... 89
4.6 Configuring Centralized Authentication on Devices in VoyenceControl..... 90

Chapter 5: GCM 8000 Comparator Optimization.....91
5.1 Setting the Link Delay Values.....91
5.1.1 Ethernet Site Link Effects on Link Delay Values.....91
Chapter 6: GCM 8000 Comparator Operation.....93
6.1 Powering Up the GCM 8000 Comparator.....93
6.1.1 GCM 8000 Comparator Power Supply and Battery Charger LEDs.....93
6.2 Powering Down the GCM 8000 Comparator.....93
6.3 GCM 8000 Comparator LED Indicators.....94
6.3.1 GCM 8000 Comparator Service LEDs.....94
6.3.2 GCM 8000 Comparator Status and Alarm LEDs.....97
6.3.3 GCM 8000 Comparator Switch or Active/Inactive Status LEDs.....98
6.3.4 GCM 8000 Comparator Link LEDs.....99
6.3.5 GCM 8000 Comparator Power Supply LEDs.....99
6.3.6 GCM 8000 Comparator Fan Assembly LEDs.....99
6.4 CSS Status Window.....99
6.4.1 Enabling the CSS Status Window.....100
6.4.2 Functions of the CSS Status Window.....100
Chapter 7: GCM 8000 Comparator Maintenance.....103
7.1 Fan Grill Cleaning Instructions.....103
Chapter 8: GCM 8000 Comparator Troubleshooting.....105
8.1 Troubleshooting the GCM 8000 Comparator.....105
8.2 Software Troubleshooting Tools.....106
8.2.1 Troubleshooting GCM 8000 Comparator Alarms in Unified Event Manager.....107
8.2.1.1 Monitoring Links and Individual Components in Unified Event Manager.107
8.2.1.2 Analyzing Unified Event Manager Active Alarms Window.....107
8.2.2 Device Troubleshooting in Unified Network Configurator.....108
8.2.3 MOSCAD Network Fault Management.....108
8.2.4 Configuration/Service Software (CSS).....109
8.2.5 Local Password and SNMPv3 Passphrase Troubleshooting.....109
8.3 Hardware Troubleshooting Tools.....110
8.3.1 LED Indicators - Troubleshooting Mode.....110
8.4 Failure of a Trunked GCM 8000 Comparator.....110
8.5 Failure of the Active Trunked GCM 8000 Comparator.....110
8.6 Failure of Active and Standby Trunked Comparators.....111
8.7 Failure of a Conventional GCM 8000 Comparator.....111
8.8 Reset Button.....111
8.9 Motorola Solutions Support Center.....111
8.9.1 Information Necessary to Contact Motorola Solutions Support Center.....112
8.9.2 Where to Call for Service.....113

8.9.2.1 Motorola Solutions Support Center....113
8.9.3 Subcontractors....113
Chapter 9: GCM 8000 Comparator FRU/FRE Procedures....115
9.1 Required Tools and Equipment....115
9.2 Field Replaceable Units (FRUs)....115
9.3 Replacing the GCM 8000 Comparator Module....116
9.4 Replacing the Fan Assembly....120
9.5 Replacing the Power Supply....121
9.6 Replacing the Backplane....122
Chapter 10: GCM 8000 Comparator Disaster Recovery....127
10.1 Recovering the GCM 8000 Comparator....127
10.2 Performing a Site Download....127

This page intentionally left blank.

List of Figures

Figure 1: GCM 8000 Comparator – Front View....25
Figure 2: GCM 8000 Comparator – Rear View....25
Figure 3: GCM 8000 Comparator – Front (Fan Assembly Removed)....26
Figure 4: Fan Module....33
Figure 5: Power Supply....34
Figure 6: AC/DC Power Distribution - GCM 8000 Comparator....35
Figure 7: Power Supply Connections (Rear)....37
Figure 8: Warning Label on Hot Modules....41
Figure 9: GCM 8000 Comparator Mounted in Rack....52
Figure 10: Battery Temperature Sensor Example 1....55
Figure 11: Battery Temperature Sensor Example 2....56
Figure 12: Front Ports - GCM 8000 Comparator....57
Figure 13: Rear Ports - GCM 8000 Comparator....58
Figure 14: GCM 8000 Comparator Auxiliary Power Wiring....59
Figure 15: VoyenceControl Welcome Page....66
Figure 16: VoyenceControl Login Window....66
Figure 17: VoyenceControl Dashboard....67
Figure 18: SNMPv3 Security Level Option Prompt....72
Figure 19: CSS Login Banner....73
Figure 20: CSS Login Banner....75
Figure 21: SNMPv3 Passphrase Prompt....81
Figure 22: Remote Access Configuration Tab....87
Figure 23: Password Configuration Window....88
Figure 24: GCM 8000 Comparator – Status Panel Screen....100
Figure 25: GCM 8000 Comparator – Status Panel Subsite Screen....101
Figure 26: GCM 8000 Comparator – Status Panel History Screen....101
Figure 27: MOSCAD Network Fault Management – Example....108
Figure 28: Fan Assembly....121
Figure 29: Power Supply....122
Figure 30: Fan Cable Connector....124

This page intentionally left blank.

List of Tables

Table 1: Operating and Environmental Specifications for the GCM 8000 Comparator..... 31
Table 2: ON/OFF Switch - States for Power Supply and Battery Charger..... 36
Table 3: Power Supply Module Backplane Connections..... 36
Table 4: Activities for Site Preparation..... 43
Table 5: Heavy Gauge Wire Resistance Examples..... 47
Table 6: Input Power Wiring..... 51
Table 7: Front Ports - GCM 8000 Comparator..... 57
Table 8: Rear Ports - GCM 8000 Comparator..... 58
Table 9: GCM 8000 Comparator Power Supply and Battery Charger LEDs..... 93
Table 10: Trunked GCM 8000 Comparator Service GREEN LEDs..... 94
Table 11: Trunked GCM 8000 Comparator Service AMBER LEDs..... 94
Table 12: Trunked GCM 8000 Comparator Service RED LEDs..... 95
Table 13: Conventional GCM 8000 Comparator Service GREEN LEDs..... 96
Table 14: Conventional GCM 8000 Comparator Service AMBER LEDs..... 96
Table 15: Conventional GCM 8000 Comparator Service RED LEDs..... 97
Table 16: GCM 8000 Comparator Status and Alarm LED Assignment..... 97
Table 17: GCM 8000 Comparator Status/Alarm LEDs Definitions..... 98
Table 18: GCM 8000 Comparator Active/Inactive Status LEDs..... 98
Table 19: GCM 8000 Comparator Active/Inactive LEDs 98
Table 20: GCM 8000 Comparator Link LEDs..... 99
Table 21: GCM 8000 Comparator Power Supply LEDs..... 99
Table 22: GCM 8000 Comparator Fan Assembly LEDs..... 99
Table 23: GCM 8000 Comparator – General Troubleshooting..... 105
Table 24: GCM 8000 Comparator Diagnostic Options..... 107
Table 25: Local Password and SNMPv3 Passphrase Troubleshooting..... 109
Table 26: GCM 8000 Comparator Field Replaceable Units..... 115
Table 27: GCM 8000 Comparator Part Numbers..... 116

This page intentionally left blank.

List of Processes

Equipment Installation Process Overview 39
Installing Device Software Prerequisites 59
Installing Devices in the UNC 62
Discovering a Device in the UNC 71
Initial Configuration of a Device in CSS 73
CSS Configuration Parameters for a Trunked GCM 8000 Comparator 88
CSS Configuration Parameters for a Conventional GCM 8000 Comparator 89
Configuring Centralized Authentication on Devices in VoyenceControl 90
Recovering the GCM 8000 Comparator 127

This page intentionally left blank.

List of Procedures

Mounting Cabinets or Racks to a Floor 45
Mounting the GCM 8000 Comparator 53
Bonding and Grounding General Requirements 53
Discovering a Device in the UNC 63
Loading Device OS Images to the UNC 64
Enabling FTP Service 65
Transferring and Installing the OS Image 66
Inspecting Device Properties for Transferred and Installed Software 68
Disabling FTP Service 69
Connecting Through a Serial Port Link 74
Setting the Device IP Address and Pairing Number in CSS 75
Setting the Serial Security Services in CSS 77
Resetting SNMPv3 User Credentials to Factory Defaults in CSS 78
Connecting Through an Ethernet Port Link 78
Setting the BR/CM Pairing Number in CSS 81
Setting the Date and Time in CSS 82
Changing SNMPv3 Configuration and User Credentials in CSS 82
Adding or Modifying an SNMPv3 User in CSS 85
Performing an SNMPv3 Connection Verification in CSS 85
Customizing the Login Banner in CSS 85
Setting the SWDL Transfer Mode in CSS 86
Setting the Local Password Configuration in CSS 87
Setting the Link Delay Values 91
Powering Up the GCM 8000 Comparator 93
Powering Down the GCM 8000 Comparator 93
Enabling the CSS Status Window 100
Replacing the GCM 8000 Comparator Module 116
Replacing the Fan Assembly 120
Replacing the Power Supply 121
Replacing the Backplane 122
Performing a Site Download 127

This page intentionally left blank.

About GCM 8000 Comparator

This manual provides an introduction to the GCM 8000 Comparator and includes procedures for installing and configuring the GCM 8000 Comparator.

This manual is intended to be used by technicians and system operators as a resource for understanding and installing the GCM 8000 Comparator after they have attended the Motorola Solutions formal training. The manual should be used in conjunction with the ASTRO® 25 system documentation and *Standards and Guidelines for Communication Sites*.

What Is Covered In This Manual?

This manual contains the following chapters:

- GCM 8000 Comparator Description on page 25 provides a description of the GCM 8000 Comparator.
- GCM 8000 Comparator Theory of Operation on page 33 provides additional explanation of the functions and connectors of the GCM 8000 Comparator.
- GCM 8000 Comparator Installation on page 39 provides installation information for the different hardware configurations of the GCM 8000 Comparator.
- GCM 8000 Comparator Configuration on page 71 provides configuration information for the GCM 8000 Comparator using the Configuration/Service Software and the Unified Network Configurator.
- GCM 8000 Comparator Optimization on page 91 provides optimization information for the GCM 8000 Comparator.
- GCM 8000 Comparator Operation on page 93 provides operations information for the GCM 8000 Comparator.
- GCM 8000 Comparator Maintenance on page 103 provides maintenance information for the GCM 8000 Comparator.
- GCM 8000 Comparator Troubleshooting on page 105 provides troubleshooting information for the GCM 8000 Comparator and the different systems supported by its hardware configurations.
- GCM 8000 Comparator FRU/FRE Procedures on page 115 provides information and procedures for replacing Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) for the GCM 8000 Comparator.
- GCM 8000 Comparator Disaster Recovery on page 127 provides references and information that will enable you to recover a GCM 8000 Comparator in the event of a failure.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Refer to the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. This may be purchased by CD 9880384V83, by calling the North America Parts Organization at 800–422–4210 (or the international number at 302–444–9842.
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Dynamic System Resilience	Provides all the information required to understand, operate, maintain, and troubleshoot the Dynamic System Resilience feature.
Conventional Operations	Provides all the information required to understand and operate the conventional GCM 8000 Comparator in a Centralized or Distributed Conventional Architecture.
MLC 8000 Configuration Tool User Guide	Provides information about an application used for configuration, analog voting display, and analog voting control of the MLC 8000 device, functioning as an analog conventional comparator for analog IP-based simulcast and non-simulcast voting, and as a subsite link converter for conventional analog, digital, and mixed mode channels.
Trunked IP Simulcast Subsystem Prime Site	Proves the information required to understand and operate the GCM 8000 Comparator in an ASTRO® 25 trunked system.

Chapter 1

GCM 8000 Comparator Description

This chapter provides a high-level description of GCM 8000 Comparator and the function it serves on your system.

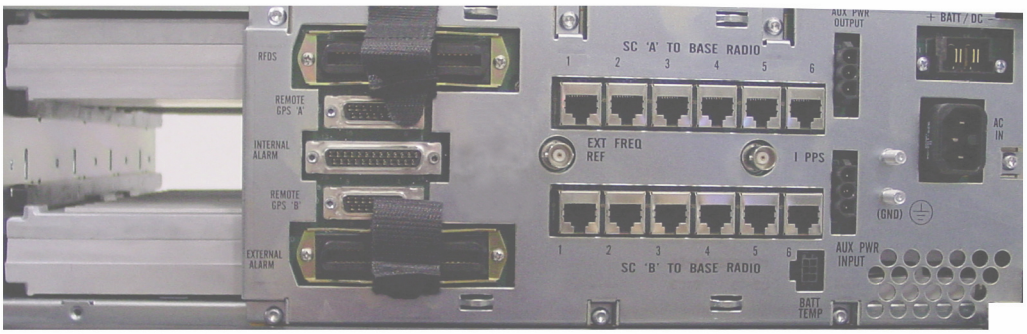
1.1 What Is the GCM 8000 Comparator?

The GCM 8000 Comparator is comprised of one or two comparator modules per chassis that support a digital IP interface or V.24 interface through a circuit link converter.

Figure 1: GCM 8000 Comparator – Front View

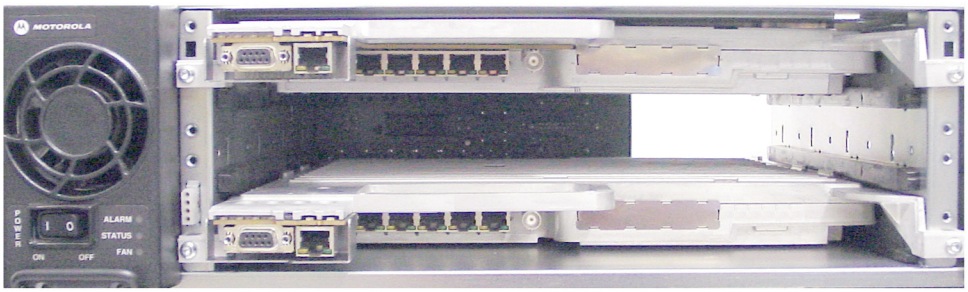
GCM 8000_Comparator_Front

Figure 2: GCM 8000 Comparator – Rear View



GCM8000_Comparator_rear1

Figure 3: GCM 8000 Comparator – Front (Fan Assembly Removed)



GCM8000_Comparator_Front_wo_cover

1.2

Supported System Configurations

The GCM 8000 Comparator is available for the following system configurations:

- Trunked IP Simulcast Prime Site
- Trunked IP Simulcast with Receive-only Site
- Trunked IP Single Transmitter Receiver Voting Site
- Centralized Conventional Architecture
  - IP Simulcast Prime Site with Trunked Conventional Channels
  - Dispatch Console Site with Colocated Conventional Channels
  - Conventional Voting Prime Site
- Distributed Conventional (Subsystem) Architecture
  - Conventional Hub Site
- ASTRO® 3.1 Conventional System
- Digital Conventional or Mixed-Mode System

1.3

GCM 8000 Comparator Functions

The GCM 8000 Comparator performs payload distribution by way of an IP network or V.24 network topologies.

The comparator can perform the following functions:

- Simulcast (trunked and conventional)
- Voting (trunked and conventional)
- Multicast (conventional)
- Data Steering (trunked and conventional)
- Console Interface (conventional)
- Redundancy Function (trunked)
- License Auditing

NOTICE: For information on mixed mode simulcast and/or voting, see the *MLC 8000s - Quick Guide for Implementing*.

In trunked operation, the comparator receives Inbound Signaling Packets (ISPs) from remote or colocated subsite base radios (ultimately received from subscriber radios through the RF). The comparator copy rejects these ISPs, forwarding only the first received copy onwards to the site controller. Additionally, the comparator controls the sequencing of the Outbound Signaling Packets (OSPs) received from the site controller when transmitting to the remote or colocated subsite base radios for transmission on the control channel. On voice and data channels, the comparator controls the creation and sequencing of the embedded or standalone link control information (based on messages received from the site controller), that is sent out on the channel providing extra control information to subscriber radios using that voice or data channel. The comparator also supports fallback states when communication to the site controller or between the site controller and the zone controller is lost or limited.

NOTICE: Site trunking and Failsoft modes of operation are supported for fallback operation. See the Troubleshooting chapter.

1.3.1
Simulcast Function

The simulcast function (trunked or conventional) is performed when multiple base radios in separate locations broadcast the same signal on the same frequency at the same time (simultaneously). This function helps to ensure that a particular geographic area (typically comprised of physical barriers such as mountains, buildings, and other barriers) is covered. The comparator module receives an absolute time reference (1 pulse per second) from a local Global Navigation Satellite System (GNSS) receiver and uses this time reference to generate the simulcast launch time values. The comparator module embeds these simulcast launch time values into the packets that are sent to the remote site base radios. This launch time instructs the base radios at the remote sites to launch the packet at the same precise time, enabling the simulcast operation. To select the best quality audio signal, the site employs a voting operation.

For a Multi-Site Single Transmitter, Receiver Voting subsystem (with only a single transmitter) supporting FDMA-only voice and IV&D data operation, simulcast function of time launching of signals from multiple transmitters does not apply because an STRV subsystem has only a single transmitter. The comparator does not require a Simulcast Site Reference for the time reference (1 pulse per second) and the transmit launch time is not assigned. To support TDMA or Enhanced Data operation in a trunked IP Single Transmitter, Receiver Voting subsystem, launchtimes are used to provide the time alignment required for TDMA voice or Enhanced Data in the base radios. The Simulcast Site Reference is required (even with a single transmitter) to provide the time reference to the comparators for generating the launch time.

1.3.2
Voting Function

The voting function is required for simulcast operation (trunked or conventional), but can be used without simulcast in a conventional or trunked topology.

Voting function is performed when multiple base radio receivers, operating on the same frequency in separate locations, receive a subscriber radio transmission signal and route the signals to a voting comparator. The comparator processes (compares or votes) the audio received from the multiple base radio to establish a best quality composite signal to be used for transmission (simulcast transmission or non-simulcast transmission).

The voting function (comparing signals received from those multiple base radios establishes the best quality outbound signal for transmission) is independent from the method used for transmission. While simulcast employs a voted signal, a voted (or composite) signal can also be transmitted on a single base radio transmitter (non-simulcast transmission).

1.3.3
Multicast Function

Multicast function (conventional only) is performed when multiple base radios can transmit and receive, operating on different frequencies, and can still receive copies of the same voice or data from the comparator. To implement multicast function, the site employs (requires) a voting operation to establish the best quality signal for transmission.

1.3.4
Data Steering

Data steering for conventional only is performed when the inbound data request of a subscriber radio is sent to the comparator by the base radio. The comparator then forwards the identity of the best voted base radio to the Packet Data Gateway (PDG) so the outbound data response from the Customer Enterprise Network (CEN) can be routed to the appropriate base radio and then transmitted to the subscriber radio.

Data steering for simulcast occurs when the system transmits payload data packets only at the most recently recorded transmit remote sites. Data steering requires that the comparator know the best remote site for each subscriber on the packet data channel. The information is gathered from inbound messages from the subscriber on the control channel (trunked channels only) and from inbound data and responses on the packet data channel (trunked and/or conventional). All messages are sent to all remote sites, but addressed to only one remote site which causes all but one of the simulcast base radios to ignore the message. This creates the effect of site steering to a single transmitter. Messages are still time launched as when simulcasting packets, to allow the comparator to retain control, and keep a common pacing engine in the comparator.

The comparator selects the appropriate remote site that actually sends data packets over the air and it multicasts packet data payload to all connected base radios and receivers. This means that all base radios/receivers receive all packets, even if they are not going to transmit them. When sending packet data payload in a conventional IP simulcast, multicast, or Trunked IP Simulcast or Single Transmitter, Receiver, Voting (STRV) subsystem, the comparator fills in the subsite number of the base radio recorded as the best transmit remote site for the CAI ID to which the data payload is addressed.

For simulcast operation in a trunked or conventional IP subsystem, when sending packet data payload XIS messages to the base radio, the comparator indicates the simulcast launch time of the message in the first PDU XIS frame. If the comparator is to send packet data payload to a subscriber unit but does not have an associated remote site address in its database, the comparator indicates that the data payload is simulcasted.

1.3.5
Console Interface

The conventional comparator can interface to conventional base radios for supporting console management functions. The conventional comparator can also provide connectivity to the MCC 7500/7100 Console through an MCC 7500 AUX I/O Server for supporting voting control commands and conventional comparator status information.

1.3.5.1
MCC 7500 AUX I/O Server

The MCC 7500 AUX I/O Server supports virtual auxiliary inputs and outputs and is the gateway between the MCC 7500/7100 Console and the conventional comparator. The MCC 7500 AUX I/O Server provides control voting commands received from MCC 7500/7100 Consoles to a conventional comparator. The MCC 7500 AUX I/O Server also provides status information received from a conventional comparator to one or more MCC 7500/7100 Console users.

1.3.5.2
MCC 7500 Console

The MCC 7500 Console makes no differentiation between physical versus virtual AUX I/O. The console uses existing AUX I/O functionality to provide the capability for the console to interface to a conventional comparator through the MCC 7500 AUX I/O Server in order to initiate voting control commands and receiving status information.

1.3.6
Redundancy Function

In an IP simulcast prime site configured for comparator redundancy, two redundant comparator modules provide for a single channel. The two redundant comparators, operate in an active/standby configuration for protection against a single comparator or LAN switch failure at the site. One module acts as the active comparator and the second module as the standby comparator. Upon failure of an active comparator or failure of a LAN switch, the associated standby comparators become active.

If unavailable comparators were previously active, the associated standby comparators that are attached to a different LAN switch become active. Any failed voice/data channels using the unavailable comparators recover to operational after the switchover.

The active comparator manages operations at the site and sends a periodic heartbeat message to the standby comparator every 500 msec. The standby comparator monitors the periodic heartbeat messages from the active comparator. When a component fails (LAN switch or comparator), the standby comparator becomes active when it detects the failure of the active comparator.

During the switchover process, the newly active comparator must transit through the initialization process. Any calls on the failed comparator or LAN switch are interrupted or terminated. Channels using any active comparators connected to other operating LAN switches continue undisturbed. If a subscriber radio remains keyed on a failed channel during the switchover, the base radio can enter Illegal Carrier state as it does for existing Illegal Carrier scenarios or enter Local Failsoft mode, depending on how the base radio is configured.

In a Trunked IP Simulcast Prime Site Geographic Redundancy (TPSGR) subsystem, redundancy of the comparators is split between two separate sites. During normal operation, the redundant preferred comparator at the primary prime site is the active comparator for the channel. The redundant non-preferred comparator only activates upon losing communication with the redundant preferred comparator at the primary prime site. When communication is restored between the redundant comparators, the redundant preferred comparator at the primary prime site becomes the active comparator, unless a call is already in progress on the redundant non-preferred comparator. The redundant preferred comparator returns to active status once the channel becomes idle.

If the redundancy value of the comparators is incorrectly configured in a TPSGR subsystem, improper operation or suboptimal operation may result. The comparator reports a configuration error when an improperly configured redundant comparator is detected. To ensure that this type of failure does not occur, only one comparator of the pair should be designated as **Redundant Preferred**.

Valid redundancy configuration combinations for TPSGR subsystems and non-TPSGR subsystems are:

- Redundant – Redundant
- Redundant Preferred – Redundant Non-Preferred
- Redundant Non-Preferred – Redundant Preferred

NOTICE: For geographically redundant prime sites, only one comparator of the pair is configured “redundant preferred”. If either comparator is not configured to the proper redundancy value, improper operation may result.

The redundancy function of the comparators is configured through Configuration/Service Software (CSS) and Unified Network Configurator (UNC). All configuration parameters of each redundant pair of

comparators must be kept in sync manually using CSS. Status of the redundancy state or when a standby comparator fails is reported to the system manager through CSS, UNC, Unified Event Manager (UEM), or MOSCAD.

1.3.7
License Auditing

License auditing for ASTRO® 25 G-series devices at M and L core systems can be enabled through the License Manager to ensure that site licenses have been purchased and also to prevent the transfer of site licenses across systems.

The License Manager performs the following functions:

- Monitors the number of site devices in use within the system.
- Audits the number of active licenses.
- Displays a noncompliance notification on the Unified Event Manager (UEM) when the number of devices exceeds the licenses.

If a site license is not present, the following functions do not occur:

- Send or receive audio
- Vote audio
- Implement site control functions; such as assigning channels or calls.

Any issues with an existing site license are sent to the UEM without system functionality being restricted.

1.4
Subsite Topology

Comparators within a trunked system can support topologies of up to 32 subsites for voting, simulcast, and data steering functions, depending primarily on the transport bandwidth capacity available.

Conventional comparators can support topologies of up to 64 subsites for voting, simulcast, multicast, data steering, and console interface functions.

NOTICE: Conventional comparators that are colocated and share a network with a trunked IP simulcast subsystem are limited to topologies of up to 32 subsites.

1.5
How Does a GCM 8000 Comparator Work?

Each module in the comparator chassis can be assigned as a voice, data, or control channel.

It receives the following packets all through the IP network (through a single IP/Ethernet connection from the comparator to a site LAN switch):

- Voice, data, or control packets from up to 32 or 64 remote or colocated subsites
- Voice and data packets from the zone core
- Control packets from the site controller

NOTICE: Control packets and control channels are available only in a trunked system. There is no interface between a comparator and site controller in a conventional architecture.

When assigned as a voice or data channel, the comparator produces the best composite voice or data packet from a set of copies of the same packet received from the base radios at multiple remote or colocated subsites (all servicing the same channel) by voting on code words or blocks within these packets based on BER metrics. The comparator module forwards this composite voted stream of voice

or data packets to the master site and/or back to the remote or colocated subsites, and also forwards received voice or data packets from the master site to the remote or colocated remote sites. The comparator module embeds “launchtimes” in the packets sent to the remote or colocated remote sites, so that all the remote or colocated remote site base radios (servicing the same channel) can launch the packet at the same time, and by that correctly simulcast the transmission.

When assigned as a control channel in a trunked system only, the comparator module rejects the duplicate control packets received from multiple remote or colocated remote sites, forwards only the first received copy to the site controller, and also forwards control packets received from the site controller to the remote or colocated remote sites.

The comparator module accomplishes the routing of the IP packets to the correct destinations by using the multicast IP addresses. For transmissions to the zone core, the comparator module uses multicast addresses specified by the zone controller or site controller and for transmissions to the remote or colocated remote sites or the site controller, the comparator module uses statically defined multicast addresses).

For simulcast operation, RF signals are launched at precisely the same time from all channel transmitters. Global Positioning Satellite (GPS) site reference receivers are required to time synchronize all base radios at remote or colocated subsites and the comparator. The comparator receives an absolute time reference (1 pulse per second) from a local GPS receiver, and uses this time reference to generate the simulcast launch time values. The comparator embeds these simulcast launch time values into the voice and data packets that are sent to the remote or colocated subsite base radios. This launch time instructs the base radios at the remote or colocated subsites to launch the packet at the same precise time, thereby enabling the simulcast operation.

For further information on how the comparator works in a trunked IP simulcast subsystem, see the *Trunked IP Simulcast Subsystem Prime Site* and *Trunked IP Simulcast Subsystem Infrastructure* manuals.

For further information on how the comparator works in a Centralized or Distributed conventional architecture, see the *Conventional Operations* manual.

1.6 Specifications

All equipment at the site supports operation from 90/264 VAC nominal single-phase power sources at 47/63 Hz or a 43.2-60 VDC power source or battery. The 60 VDC maximum input voltage limit includes consideration of the battery charging “float voltage” associated with the intended supply system, regardless of the marked power rating of the equipment.

CAUTION: Failure to follow this power supply guideline may result in an electric shock.

The GCM 8000 Comparator has automatic battery revert capabilities and can charge batteries from the AC power supply. The power supply includes an integrated charging system that eliminates the need for UPS. The power supply provides battery equalization.

The comparator has an internal power supply and is able to provide 29 VDC auxiliary power output as a backup power source. This allows, for example, another connected comparator chassis with a power supply failure to maintain continued operation.

Table 1: Operating and Environmental Specifications for the GCM 8000 Comparator

GCM 8000 Comparator	Specifications
Physical Dimensions:	Height: 5.25 in. (133 mm) Width: 19.0 in. (483 mm)

Table continued…

GCM 8000 Comparator	Specifications
	Depth: 18.0 in. (457 mm)
Weight:	40 lb (18 kg)
Temperature Operating Temperature: Storage Temperature:	 -30 °C to 60 °C (-22 °F to 140 °F) -40 °C to 85 °C (-40 °F to 185 °F)
Relative Humidity:	90% relative humidity at 50 °C non-condensing
Input Supply Voltage:	AC: 90–264 VAC, 47–63 Hz DC: 43.2 to 60.0 VDC (+/-48 VDC nominal)
Auxiliary Power Outputs:	28.94 V +/- 3%
Power Consumption:	• One module - AC: 130 W - DC: 60 W • Two modules - AC: 160 W - DC: 80 W
Operating Altitude:	Up to 1800 m (6000 ft) above sea level

Chapter 2

GCM 8000 Comparator Theory of Operation

This chapter explains how the GCM 8000 Comparator works in the context of your system.

2.1 GCM 8000 Comparator

The GCM 8000 Comparator chassis is comprised of one or two separate comparator modules with each module supporting one channel, a power supply, and a fan assembly.

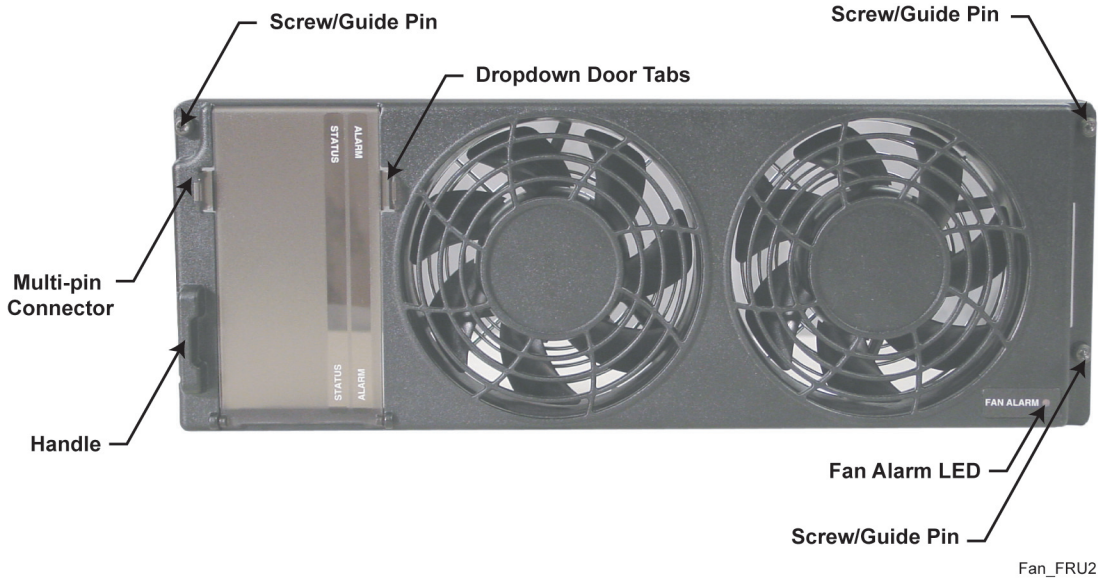
2.2 Fan Module

The fan module provides intermittent forced air cooling for the power amplifier, and comparator modules. A thermostat behind the fan module controls the fans. The fan module houses two 119 mm axial fans which deliver a total of approximately 160 cubic feet per minute of airflow. Nominal fan speed is 4100 revolutions per minute. Each fan has a built-in speed sensor which turns on the red Fan Alarm LED if the fan speed for either fan falls below 30% of the rated speed.

The fan module connects to the backplane through a 4-pin port on the front of the chassis.

NOTICE: The power supply module has its own fan which provides independent airflow.

Figure 4: Fan Module



2.3

Power Supply

Figure 5: Power Supply

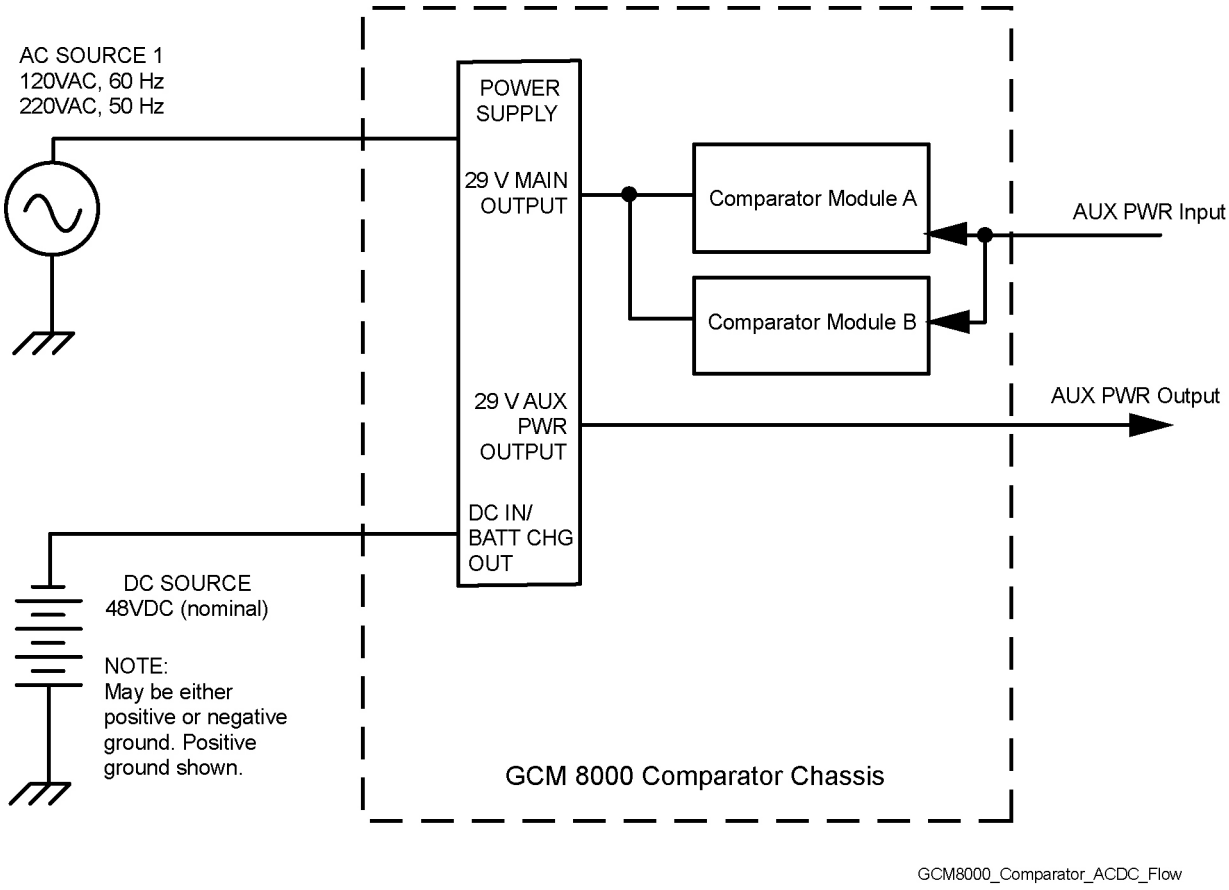
G_series_power_supply_A

The power supply operates from either an AC or DC input and provides the DC operating voltage for both the comparator modules in the chassis. When operating from an AC source (90 to 264 VAC, 47-63 Hz), the supply provides a separate battery charger, to maintain the charge on a 48 VDC nominal system, positive or negative ground, if installed. The power supply generates 2 DC output voltages of 29 V with respect to output ground. The power supply automatically adjusts to AC input ranges and supplies a steady output.

The Main DC output of the power supply is used to provide power to all comparator modules installed in that chassis. The AUX PWR INPUT AUX PWR OUTPUT should be daisy-chained between all comparator chassis.

2.3.1
AC/DC Power Distribution

Figure 6: AC/DC Power Distribution - GCM 8000 Comparator



The comparator operates on AC power as the preferred power source. When AC power is not available, the comparator switches to operate from the DC source. Operation returns to the AC source when the AC source is restored. Switch over from AC to DC and back again is fully automatic. No operator action is required.

The main DC output of the power supply is used to provide power to the comparator modules. The Auxiliary output of the power supply can be used as a power source for another comparator chassis.

2.3.2
Power Supply Battery Charger

The power supply may include an integrated battery charger. The battery charger is controlled through software residing on the associated device module. Software contains the information on supported battery types and obtains user-specific information pertaining to the particular site. The device software receives battery bus voltage and battery temperature information from the power supply, and uses these variables with supported battery charging profiles to return a signal which sets the charger output voltage appropriately. The battery charge and temperature conditions are viewed through Configuration/Service Software (CSS) and Unified Network Configurator (UNC), or through alarms to Unified Event Manager (UEM).

The maximum charging current available from the integrated charger is 3 A (48 VDC nominal system). A battery with capacity no larger than 60 Ah should be connected to a single charger to ensure that the charger maintains an adequate state-of-charge on the backup battery, and the backup battery is

restored to full capacity within a reasonable amount of time following operation on battery backup power.

In addition to standard sealed lead-acid batteries (valve-regulated lead acid or gel cells), the power supply supports charging of vented lead-acid and NiCd batteries.

2.3.3
Battery Temperature Sensor Cable

The integrated charger in the power supply performs temperature compensated battery charging when a temperature sensor is connected. If the sensor is disconnected, the charger continues to operate as an uncompensated charger with the charging profile following the minimum charger voltage specified by the battery manufacturer.

Included is a 40 ft battery temperature sensor cable, which attaches to a battery pack, supplied by your organization, and to the backplane of the device. This three-wire cable carries a voltage signal to the power supply from the sensor element, which must be mounted close to the storage battery. Voltage is proportional to the battery temperature, and the diagnostic circuitry in the power supply module. This cable is extended to a total length of 190 ft using 50 ft extensions. See Battery Temperature Sensor Mounting on page 54.

IMPORTANT: Continuous operation with a disconnected sensor is not recommended.

2.3.4
ON/OFF Switch for Power Supply and Battery Charger

This table identifies the switch states for the power supply and battery charger.

Table 2: ON/OFF Switch - States for Power Supply and Battery Charger

Switch Position	Power Supply State	Battery Charger State
ON (1)	• Power Factor Correction (PFC) section is active (AC input only) • Main DC converter runs to create the MAIN and AUX DC outputs	DLN6781A can be started if desired (AC input only) DLN6805A Disabled
OFF (0)	• Main DC converter is turned OFF and the MAIN and AUX DC outputs become 0.0 VDC	Disabled (AC input only)

2.3.5
Power Supply Module Backplane Connections

This table provides descriptions and functions of the power supply backplane connections.

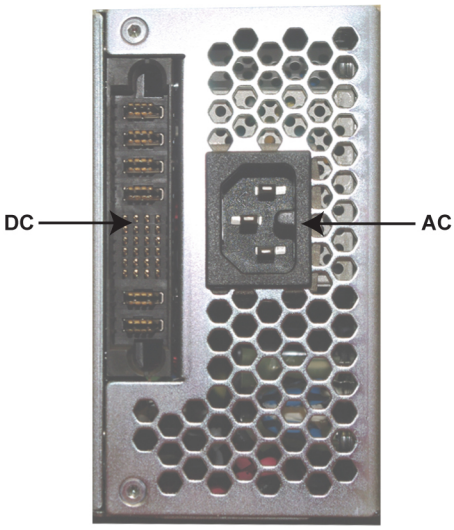
Table 3: Power Supply Module Backplane Connections

Port/Type	Description
AC	Input only

Table continued…

Port/Type	Description
Battery / DC Power and Control Signal	**48 VDC:** • Provides the DC input to the power supply when operating from a DC source. • Connects the charger output to the standby battery when operating from an AC input with a standby DC battery. **29 VDC:** • Provides the Main and Auxiliary DC outputs of the power supply for use by the power amplifier, transceiver, and site controller. Other signals this connector handles include control interface and battery temperature interface.

Figure 7: Power Supply Connections (Rear)



G_Series_PS_Rear1

2.4 Auxiliary Power

A GCM 8000 Comparator can receive a 29 VDC auxiliary power signal from the auxiliary power output from another comparator at the site or provide a 29 VDC auxiliary power signal to the auxiliary power input of another comparator at the site. See GCM 8000 Comparator Front Ports on page 57 and GCM 8000 Comparator Rear Ports on page 58.

2.5 Network Fault Management

A GCM 8000 Comparator allows for configuration and network fault management of the comparator module, the power supply and fan, and the subsite links through the SNMP communication with CSS, UEM, UNC, or MOSCAD Network Fault Management (NFM) over the 100BaseT Ethernet interface. Commands such as enable/disable can also be sent to the comparator through the UEM, UNC, or MOSCAD NFM.

NOTICE:

- Enable/Disable is not available for a conventional comparator.
- CSS is the only network management tool available for a conventional comparator in a K core site.

The Unified Event Manager (UEM) can be established as a more centralized fault management solution replacing the MOSCAD GMC. See the *Unified Event Manger* and the *UEM GMC MOSCAD Transition Guide* for details.

Chapter 3

GCM 8000 Comparator Installation

This chapter details installation procedures relating to the GCM 8000 Comparator.

3.1 Pre-Installation Tasks

Follow this process to perform the installation tasks. Ensure that you have the following:

- Appropriate cables
- Access to Software Download Manager (SWDL), Configuration/Service Software (CSS), and the Unified Network Configurator (UNC)
- IP/DNS information
- Login and password information

3.1.1 Equipment Installation Process Overview

Process:

1. Prepare the site to comply with the Motorola Solutions requirements and specifications for the equipment, as listed in the *Standards and Guidelines for Communication Sites* manual. Other codes and guidelines that may apply to the location must also be met. See General Safety Precautions on page 40.
2. Inspect and inventory all racks, cabinets, cables, and other equipment with a Motorola Solutions representative to ensure that the order is complete. See General Installation Standards and Guidelines on page 42.
3. A variety of tools are needed to install and service the equipment. If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solutions Support Center (SSC). See General Installation/Troubleshooting Tools on page 48 for a list of general recommended tools for installing and servicing the hardware.
4. Install all equipment using the site drawings and other documents provided by the Field Engineer. Use the installation standards and guidelines for placing and installing equipment.
5. Properly ground all the racks and cabinets to protect against ground faults, electrical surges, and lightning. See GCM 8000 Comparator Hardware Installation on page 50.
6. Connect all necessary cables within a rack and between the racks for system interconnection. See GCM 8000 Comparator Front Ports on page 57 and GCM 8000 Comparator Rear Ports on page 58.
7. Run a preliminary check of a site before applying power.
8. See Installing Device Software Prerequisites on page 59 for a list of items you need access to prior to installing the software.
9. See Installing Devices in the UNC on page 62 to discover the comparator and to load OS software images from the UNC.
10. See Device Configuration in CSS on page 73 to program the configurations into the comparator using CSS.

11 See Configuring Centralized Authentication on Devices in VoyenceControl on page 90 to program the comparator using UNC.

3.2 General Safety Precautions

WARNING: Compliance with FCC guidelines for human exposure to Electromagnetic Energy (EME) at Transmitter Antenna sites generally requires that personnel working at a site must be aware of the potential for exposure to EME, and can exercise control of exposure by appropriate means, such as adhering to warning sign instructions, using standard operating procedures (work practices), wearing personal protective equipment, or limiting the duration of exposure. For more details and specific guidelines, see “Appendix A” of the Motorola Solutions *Standards and Guidelines for Communications Sites* manual.

Observe the following general safety precautions during all phases of operation, service, and repair of the equipment described in this manual. Follow the safety precautions listed and all other warnings and cautions necessary for the safe operation of all equipment. See the appropriate section of the product service manual for additional pertinent safety information. Due to the danger of introducing additional hazards, do not install substitute parts or perform any unauthorized modifications of equipment.

NOTICE: The installation process requires preparation and knowledge of the site before installation begins. Review installation procedures and precautions in the Motorola Solutions *Standards and Guidelines for Communications Sites* manual before performing any site or component installation.

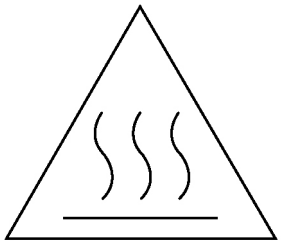
Always follow all applicable safety procedures, such as Occupational Safety and Health Administration (OSHA) requirements, National Electrical Code (NEC) requirements, local code requirements, and safe working practices. Also, all personnel must practice good judgment. General safety precautions include the following:

- Read and follow all warning notices and instructions marked on the product or included in this manual before installing, servicing, or operating the equipment. Retain these safety instructions for future reference.
- If troubleshooting the equipment while power is on, be aware of the live circuits.
- Do not operate the radio transmitters unless all RF connectors are secure and all connectors are properly terminated.
- Ground all equipment properly in accordance with the Motorola Solutions *Standards and Guidelines for Communications Sites* manual and specified installation instructions for safe operation.
- Slots and openings in the cabinet are provided for ventilation. Do not block or cover openings that protect the devices from overheating.
- Only a qualified technician familiar with similar electronic equipment should service equipment.
- Some equipment components can become hot during operation. Turn off all power to the equipment and wait until sufficiently cool before touching.
- Maintain emergency first aid kits at the site.
- Direct personnel to call in with their travel routes to help ensure their safety while traveling between remote sites.
- Institute a communications routine during certain higher risk procedures where the on-site technician continually updates management or safety personnel of the progress so that help can be dispatched if needed.
- Never store combustible materials in or near equipment racks. The combination of combustible material, heat, and electrical energy increases the risk of a fire safety hazard.
- Equipment installed at the site meeting the requirements of a "restricted access location," per UL60950-1, is defined as follows: "Access can only be gained by service persons or by a user who

has been warned about the possible burn hazard on equipment metal housing. Access to the equipment is by using a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location."

WARNING: Burn hazard. The metal housing of the product may become extremely hot. Use caution when working around the equipment.

Figure 8: Warning Label on Hot Modules



warning_hot

WARNING: DC input voltage must be no higher than 60 VDC. This maximum voltage includes consideration of the battery charging "float voltage" associated with the intended supply system, regardless of the marked power rating of the equipment. Failure to follow this guideline may result in electric shock.
RF energy burn hazard: disconnect power in the cabinet to prevent injury while disconnecting and connecting antennas.

CAUTION: All Tx and Rx RF cables outer shields must be grounded per Motorola Solutions *Standards and Guidelines for Communications Sites* manual requirements.
All Tx and Rx RF cables must be connected to a surge protection device according to the Motorola Solutions *Standards and Guidelines for Communications Sites* manual. Do not connect Tx and Rx RF cables directly to an outside antenna.

IMPORTANT: All equipment must be serviced by Motorola Solutions-trained personnel.

3.2.1
DC Mains Grounding Connections

CAUTION: This equipment is designed to permit the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment. If this connection is made, you must meet all following conditions:

- Connect this equipment directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus in which the DC supply system earthing electrode conductor is connected.
- Locate this equipment in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor (and also the point of earthing of the DC system). Do not earth the DC system elsewhere.
- Locate the DC supply source within the same premises as the equipment.
- Do not install switching or disconnecting devices in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

3.2.1.1
Disconnect Device Permanently Connected

Incorporate a readily accessible disconnect device (circuit breaker or switch) in the building installation wiring.

3.2.1.2
Multiple Power Source

This product has multiple power sources. If service requires the removal of a power source, disconnect all inputs (AC and DC powers) to remove power completely to the equipment before servicing.

3.2.1.3
Connection to Primary Power

For supply connections, use wires suitable for at least 75 °C.

3.2.1.4
Replaceable Batteries

WARNING: Risk of Explosion if you replace the battery with an incorrect type. Dispose of used batteries according to the instructions.

3.2.2
Maintenance Requiring Two People

Identify maintenance actions that require two people to perform the repair. Two people are required when:

- A repair has the risk of injury that would require one person to perform first aid or call for emergency support. An example is work around high-voltage sources. If an accident occurs to one person, another person may be required to remove power and call for emergency aid.
- Heavy lifting is involved. Use the National Institute of Occupational Safety and Health (NIOSH) lifting equation to determine whether one or two persons are required to lift a system component when it must be removed and replaced in its rack.

3.2.3
Equipment Racks

Lift equipment racks without the use of lifting equipment only when sufficient personnel are available to ensure that regulations covering health and safety are not breached. Use an appropriately powered mechanical lifting apparatus for moving and lifting the equipment racks. In addition to these points, comply with any local regulations that govern the use of lifting equipment.

WARNING: Crush Hazard could result in death, personal injury, or equipment damage. Equipment racks can weigh up to 360 kg (800 lb). See the following instructions for proper lifting procedures.

3.3
General Installation Standards and Guidelines

This section provides several guidelines to ensure a quality install. Review these guidelines before unpacking and installing the system. Additionally, review the installation information in the *Standards and Guidelines for Communication Sites* manual for more details, including:

- Equipment installation
- Antenna installation

You should also review installation information specifically for GCM 8000 Comparator and subsystems in GCM 8000 Comparator Hardware Installation on page 50.

3.3.1
General Site Preparation Overview

Perform the activities listed in this table to ensure proper site preparation. The table references specific chapters in the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for more information.

Table 4: Activities for Site Preparation

Activity	Description of Activity	Chapter Reference
Review the site plan.	• Prevents potential on-site and off-site interference by local trunked systems. • Minimizes cable lengths. • Determines the location of telecom equipment.	• Chapter 2 "Site Design and Development"
Determine site access and security.	Outlines of site access and security measures.	• Chapter 2 "Site Design and Development"
Review safety considerations.	Outlines general, installation, and environmental safety guidelines and requirements and OSHA-related considerations.	• Chapter 3 "Communications Site Building Design and Installation"
Schedule installation of telephone service.	Ensures options and functions of on-site, two-way communications for personnel safety and maintenance.	• Chapter 3 "Communications Site Building Design and Installation"
Review grounding specifications.	Ensures that the site meets or exceeds the Quality Audit Checklist in Appendix F as well as the Power and Grounding Checklist in Appendix D.	• Appendix D. “Grounding (Earthing) Electrode System Testing/ Verification” • Appendix F. “R56 Compliance Checklist”
Schedule installation of site power.	Covers grounding, power sources, and surge protection.	• Chapter 4 "External Grounding (Earthing)" • Chapter 5 "Internal Grounding (Earthing)" • Chapter 6 "Power Sources" • Chapter 7 "Surge Protective Devices"

3.3.2
General Equipment Inspection and Inventory Recommendations

Take an inventory of all equipment with a Motorola Solutions representative to ensure that the order is complete. Carefully inspect all equipment and accessories to verify that they are in good condition. Promptly report any damaged or missing items to a Motorola Solutions representative.

CAUTION: Do not tamper with factory configuration settings for these devices. These settings include software configuration, firmware release, password, and physical connections. Motorola Solutions has configured and connected these devices to meet specific performance requirements. Tampering with these devices may result in unpredictable system performance or catastrophic failure.

3.3.3
General Placement and Spacing Recommendations

When placing equipment at a site, perform the following:

- Place each rack on a firm, level, and stable surface, and bolt the racks together.
- Use correct mounting hardware and shims to prevent rack movement.
- Use strain relief when installing and positioning cables and cords to help ensure that no interruption of service occurs.
- Provide an appropriate amount of space around all components to allow for proper air flow, cooling, and safe access to equipment.
- Locate the site racks and other equipment with enough spacing to allow access for service.

  NOTICE: Proper spacing of equipment is essential for ease of maintenance and safety of personnel. Spacing requirements have been established to meet the National Fire Protection Associations (NFPA) code, and the American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) standards. Adhere to any local regulations that apply to the installation.
- Locate the system in an area free of dust, smoke, and electrostatic discharge (ESD).
- See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for details on these space requirements.

3.3.4
General Cabinet Bracing Recommendations

Use all supplied bracing hardware when installing a rack or cabinet, and secure all equipment within a rack or cabinet.

If additional equipment is installed, see the system design document the field engineer provided, or consult the Motorola Solutions Field Representative.

Subsystem cabinets are self-supporting structures. In areas subject to seismic activity, additional bracing of the cabinet may be required to prevent it from tipping. However, the bracing hardware must be locally procured. No specific procedures are provided within this manual for bracing cabinets in active seismic areas. See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for details on seismic conditions.

3.3.5
Mounting Cabinets or Racks to a Floor

When and where to use: Perform the following steps to properly install a cabinet or open rack within a site building. Secure the cabinets and racks to the floor for optimum stability. This procedure is written so that the cabinet or rack is moved only once.

Procedure:

1. Carefully mark the mounting holes with a pencil, as indicated on the appropriate cabinet or rack footprint.
2. Drill the marked mounting holes to the appropriate depth of the mounting hardware with a hammer drill and bit.
3. Insert an anchor into the drilled hole. If necessary, tap the anchor into place using a hammer.
4. For cabinets, remove the four screws securing the bottom kick panel to the front and back of the cabinet. Remove the kick panel and set aside during installation.
5. Carefully move the cabinet or rack into the position indicated by the holes in the floor.

   WARNING: Equipment cabinets and racks are heavy and may tip. Use extreme caution when moving. Lift from top eyenuts with the appropriate apparatus, or secure the cabinet or rack from tipping if lifting from the bottom. Failure to do so could result in death or serious injury or equipment damage.
6. Adjust and level the cabinet or rack as necessary to position the cabinet mounting holes with the pre-drilled holes.
7. Secure the cabinet or rack to the site floor with the locally procured mounting hardware.

   IMPORTANT: If securing the cabinet or rack to a concrete floor, use 1/2-inch grade 8 bolts with anchors.

3.3.6
General Bonding and Grounding Requirements

Cabinets and racks include a Rack Grounding Bar (RGB) with the capacity to terminate numerous ground wires. Attach equipment added to the cabinet or rack to the ground bar using solid or stranded 6 AWG copper wire.

The RGB uses dual-hole lugs to terminate ground wires. The minimum number of dual-hole attachments is system-dependent and specified by the customer. This bar provides electrical continuity between all bonds and ground wire with a current-carrying capacity equal to or exceeding that of a 6 AWG copper wire.

See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for more information on proper bonding and ground at a site.

3.3.7
General Cabling Requirements

Diagrams for cabling are typically included in the system-specific configuration documentation Motorola Solutions provides. Also see the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for cabling standards.

IMPORTANT: System certification was completed using shielded cables. To prevent emission problems, use only shielded cables. Do not substitute other cable types.

- Position the equipment to avoid excessive tension on cables and connectors. Cables must be loose with absolutely no stress on the connectors. Careful cable routing and securing the cables with tie wraps (or other devices) is one way to provide this protection. Set up preventive maintenance loops .
- Dress the cables neatly using cable ties. Do not tighten the cable ties until you are sure that the required service length and bend radius requirements are met. Leave cable ties loose enough to allow adjustment.
- Verify that all cables are properly labeled to match System-specific configuration documentation Motorola Solutions provided.
- Ensure that cables do not exceed the minimum bend radius as outlined in the Motorola Solutions *Standards and Guidelines for Communication Sites* manual.

CAUTION: Use only Category 5 Shielded Twisted Pair (or higher) for cabling Ethernet connections. Motorola Solutions has engineered this system to meet specific performance requirements. Using other cabling and connectors may result in unpredictable system performance or catastrophic failure.

NOTICE: For more information on cabling guidelines, see the documentation supplied with components from each equipment manufacturer.

3.3.8
General Power Guidelines and Requirements

See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for information on providing electrical service, power budgeting, selecting batteries, and other topics for supplying power at the site.

Perform electrical installation work in accordance with the current edition of the NFPA 70 and local building codes. Where required, use a qualified and licensed electrician for all electrical installations.

3.3.8.1
General AC Power Guidelines and Requirements

The Motorola Solutions *Standards and Guidelines for Communication Sites* manual defines the guidelines and requirements for cabinets and racks which house equipment that requires AC power input. Some of the guidelines and requirements are as follows:

- The cabinet or rack is designed to accept 120/240 V, single-phase power with an amperage service size as required by the electronic equipment.
- Cabinets and racks powered by commercial power must be equipped with a Nationally Recognized Test Laboratory (NRTL) certified power distribution module that contains a main circuit breaker or individual circuit breakers of the correct size as required for the electronic equipment or as the customer specified.
- A decal showing an electrical schematic of the power wiring is affixed to the inside surface of the cabinet.
- All AC power equipment and electrical components must conform to National Electrical Manufacturers Association (NEMA) and National Electrical Code (NEC). The AC power equipment must also be listed by an NRTL.
- A surge arrestor, designed to protect equipment systems from a 120/240 V service and load center, is placed on the power feed ahead of all individual load center circuit breakers. This gapless arrestor must be listed by an NRTL for the purpose intended.

- Selection of a surge arrestor is based on the susceptibility of the equipment powered by the electrical service, with margin provided for locally generated disturbances. See ANSI/IEEE C62.41 (21) for more details.
- At least one 120 VAC, 15 A duplex convenience outlet equipped with Ground Fault Interrupter (GFI) protection must be provided in the electronic equipment compartment.

CAUTION: Do not use surge/transient suppressors without careful and expert power system analysis.

NOTICE: Redundant devices could be terminated on different AC main phases so that a single phase failure does not result in a power loss for both devices.

3.3.8.2
General Breaker Recommendations

Each power supply should have its own supply breaker to ensure that a fault which causes the breaker to open does not result in the loss of multiple transmit channels. The breaker recommendations for AC and DC supply breakers are as follows:

- For a 120 VAC, 60 Hz application, the AC supply breaker should be rated for a continuous current of 20 A. For a 220 VAC, 50 Hz application, the AC supply breaker should be rated for a continuous current of 10 A minimum, not to exceed 20 A.
- For a 48 VDC application, the DC supply breaker must be rated for a continuous current of at least 5 A but not to exceed 25 A.

3.3.8.3
General Battery Installation Recommendations

The batteries and charger should be as close as possible to the rectifier system using the cables. A very heavy gauge stranded cable is advised to minimize voltage drop. The resistance of some heavy gauge wire is:

Table 5: Heavy Gauge Wire Resistance Examples

Gauge	Resistance
#6 gauge	0.3951 /1000 ft
#4 gauge	0.2485 /1000 ft
#2 gauge	0.1563 /1000 ft

The maximum voltage drop can be calculated by knowing the peak current drawn by the radio system. Use the following formula:

Total Voltage drop = [/1000 ft] x [total loop length (ft)] x [Ipeak (A)] + [connector(s) voltage drop(s)]

3.3.9
General Electrostatic Discharge Recommendations

Electronic components, such as circuit boards and memory modules, can be sensitive to Electrostatic Discharge (ESD). Use an antistatic wrist strap and a conductive foam pad when installing or upgrading the system.

If an ESD station is not available, wear an antistatic wrist strap. Wrap the strap around the wrist and attach the ground end (usually a piece of copper foil or an alligator clip) to an electrical ground. An electrical ground can be a piece of metal that literally runs into the ground (such as an unpainted metal pipe), or the metal part of a grounded electrical appliance. An appliance is grounded if it has a three-prong plug and is plugged into a three-prong grounded outlet.

NOTICE: Do not use a computer as a ground, because it is not plugged in during installation.

3.3.10
FCC Requirements

Radio frequency (RF) transmitters installed at sites within the US must be in compliance with the following FCC regulations:

- The station licensee is responsible for the proper operation of the station at all times and is expected to provide observations, servicing, and maintenance as often as may be necessary to ensure proper operation.
- The transmitter ERP must not exceed the maximum power specified on the current station authorization.
- The frequency of the transmitter must be checked during initial installation of the transmitter, when replacing modules, or when making adjustments that affect the carrier frequency or modulation characteristics.

This equipment has been tested and found to comply with the limits for a Class A digital device, according to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference to radio communications when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy. If not installed properly and used in accordance with the instruction manuals, the equipment may cause harmful interference to radio communications. Operation of some compliant equipment in a residential area may cause harmful interference to radio communications, in which case the interference must be corrected.

3.3.11
Networking Tools

Use the following networking tools for installing and servicing the network:

- Fluke® OneTouch Assistant LAN tester
- NiMH rechargeable battery for Fluke
- T1/E1 or E1 test set (such as the Hewlett-Packard® HP37702A)
- Serialtest® software with the ComProbe® and SerialBERT option

3.3.12
General Installation/Troubleshooting Tools

If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solutions Support Center (SSC). See Motorola Solutions Support Center on page 111.

3.3.12.1
General Tools

Use the following general tools to install, optimize, and service equipment in the system:

- 150 MHz 4 Channel Digital Storage Oscilloscope
- Transmission Test Set (TIMS Set)
- Aeroflex 3900 Series Service Monitor or equivalent
- 50 Ohm Terminated Load
- Digital Multimeter (DMM)
- Terminal Emulation Software
- DB-9 Straight through serial cable
- RS-232 Cables with Connectors
- Punch Block Impact Tool
- MODAPT – RJ-45 Breakout Box
- Remote RJ-11/ RJ-45 Cable Tester (1200 ft length maximum)
- PC Cable Tester (RG-58, 59, 62, BNC, RJ-45, RJ-11, DB-9, DB-15, DB-25, Centronics 36-pin connectors)
- ESD field service kit
- Amprobe Instruments GP-1 Earth Tester
- AEMC 3730 Clamp-on Ground Resistance Tester

3.3.12.2
Rack Tools

Use the following tools to install, optimize, and service the equipment:

- Service Monitor: Aeroflex 3900 Series Service Monitor with P25 Options installed (plus Time Division Multiple Access (TDMA) options as required)
- Personal Computer meeting the following specifications:
  - Operating Systems:
    + Windows 10 (Server 2012 R2)
- Hardware Requirements:
  - Processor:
    + 1 GHz or higher Pentium grade
  - Processor Memory:
    + 2 GB RAM recommended for Windows 10
  - Hard Disk Space:
    + 300 MB minimum free space (for a Typical Installation, including Help Text and Software Download Manager) or 100 MB minimum free space (for a Compact Installation)
  - Peripherals:
    + Microsoft Windows supported mouse or trackball
    + Microsoft Windows supported serial port for product communication
    + Microsoft Windows supported Ethernet port for product communication
    + Microsoft Windows supported printer port for report printing
    + CD-ROM for software installation
- Configuration/Service Software (CSS) DLN6455

- CSS serial programming cable
- Ethernet cable
- Antenna tester
- 50 Ohm terminated load
- Rohde & Schwarz NRT-Z14 Directional Power Sensor, 25-1000 GHz, 0.1-120 W. Recommended for all uses when a service monitor is not available.

3.3.13
Technical Support for Installation

Technical support is available from the site-specific documents the Field Engineer or Motorola Solutions Field Representative provided for the system, one of the Motorola Solutions Support Centers (SSC), or qualified subcontractors.

- SSC can help technicians and engineers resolve system problems and ensure that warranty requirements are met. Check your contract for specific warranty information. See Motorola Solutions Support Center on page 111.
- The Motorola Solutions System Service Subcontractor Assessment program ensures that service people contracted by Motorola Solutions meet strict minimum requirements before they can work on any system. For more information on this program, contact the Motorola Solutions representative.

3.3.13.1
Site-Specific Information

When the Motorola Solutions Center for Customer Solution Integration (CCSi) stages a system, the Field Engineer assigned to the system creates all site-specific system documentation to document how the system was staged. Site-specific information includes the following:

- Site design drawings showing the location of racks, cabinets, cable trays, and other components
- Rack drawings showing the location of the equipment in each rack
- Cable matrix in a table format that shows each cable and its connections
- Interconnect wiring diagrams to show the cable connections between devices
- Pre-programmed parameters of each site component
- Templates used to program each device
- All firmware and software revisions of each site component
- Test data from each device that requires operational verification
- Optimization requirements and settings of each electrical path
- Acceptance Test Plan for the site components

NOTICE: Maintain this site-specific information to reflect the current site configuration and layout for the system.

3.4
GCM 8000 Comparator Hardware Installation

This section explains the hardware installation procedures for the GCM 8000 Comparator.

3.4.1
Placement and Spacing

Cabinets and racks allow equipment to be added to a site. Always consider room for expansion when setting up a site. Cabinets or racks may be installed next to each other or to other equipment. However, provide all cabinets and racks with sufficient floor space to permit access for installation and service.

Clearance required for service and installation is at least 2 ft in the front and rear.

Front access:

- At least 2 ft floor access in front of the cabinet or rack.

Side and rear access:

- At least 2 ft floor access at the rear of the cabinet or rack, or
- At least 2 ft access on at least one side of the cabinet or rack, plus 6 inches at the rear of the cabinet or rack.

To maintain this clearance, the following is required:

- If there is less than 2 ft rear access, do not install more than two cabinets or racks side by side, and allow at least 2 ft access on at least one side of each cabinet or rack.
- For the cabinet version, if there is less than 2 ft rear access, do not install the optional rear door on the cabinet.

NOTICE: For the cabinet version, when an eyenut has to be replaced, provide at least 2 ft access to both sides of the cabinet so that both side panels can be removed.

3.4.2
Power Requirements

The standard GCM 8000 Comparator is designed with a switching power supply, that operates over a wide range of voltages (90–264 VAC) and frequencies (47–63 Hz) without any modifications or jumper changes. The power supply is enclosed in a metal case with a self-contained, thermostatically controlled cooling fan. The power supply takes up three slots in the card cage.

The front panel of each power supply module includes an on/off switch and two LED indicators, which are designed to easily show the functional status of the module.

Table 6: Input Power Wiring on page 51 lists the power connections for both DC and AC power. Follow the guidelines in the *Standards and Guidelines for Communication Sites* manual for information on providing electrical service, power budgeting, selecting batteries, and other topics for supplying power at the site.

IMPORTANT: You must provide proper strain relief for the power cable. Route and secure the power cable to protect it from strain and external forces. Careful cable routing and securing the cables with tie wraps (or other devices) is one way to provide this protection.

Table 6: Input Power Wiring

If the GCM 8000 Comparator uses	Then
AC power	Connect a power cord from the Input port on the rear of the unit to an AC outlet.
DC power	Input from a +/- 48 VDC nominal power supply.

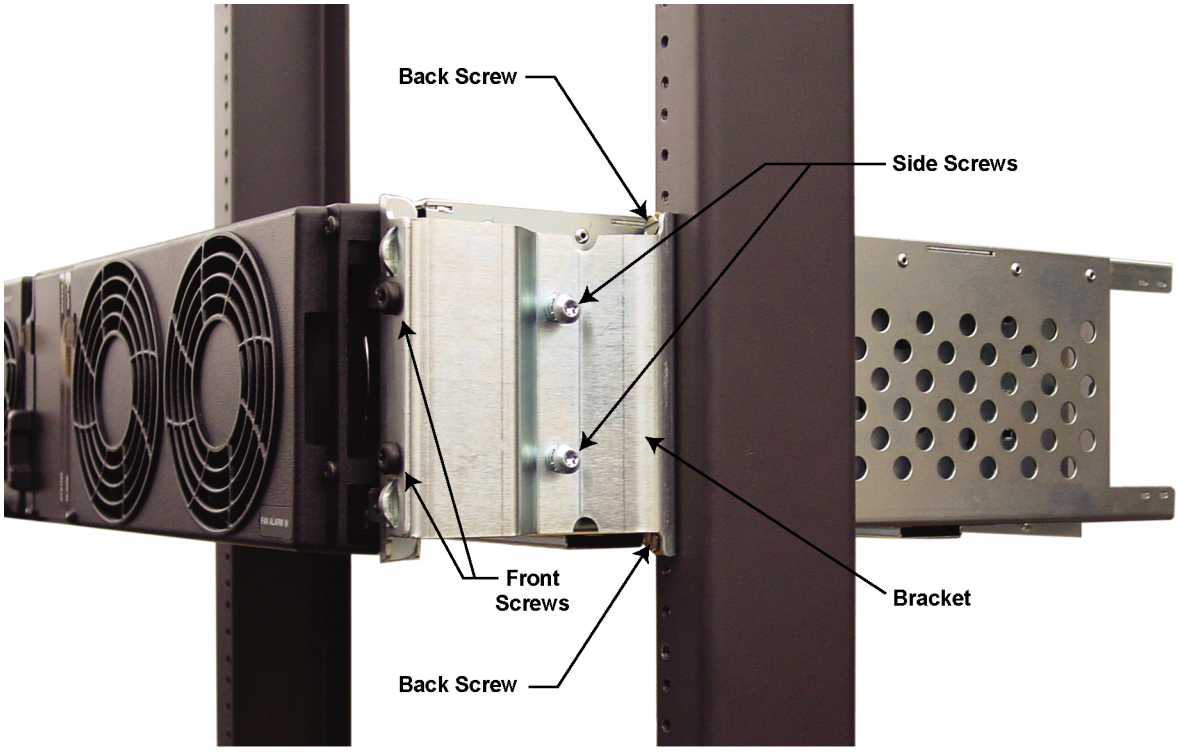
If the GCM 8000 Comparator uses	Then
	IMPORTANT: You must ground the battery system, either positive or negative, at the battery because the DC power system in the comparator floats, it is not grounded.

3.4.3
GCM 8000 Comparator Mounted in a Rack

The GCM 8000 Comparator mounts in a rack secured to the floor. For open racks, two brackets are required to distribute the weight. Without brackets, the center of gravity of the system shifts to the back, potentially causing structural issues with the rack. The brackets come with the required number of screws.

NOTICE: Redundant comparators should not be housed in the same chassis. The redundant comparators must be on separate LAN switches.

Figure 9: GCM 8000 Comparator Mounted in Rack



NOTICE: It is suggested that two people perform this installation so that one person holds the comparator in place while the other person attaches the brackets to the rack.

3.4.3.1

Mounting the GCM 8000 Comparator

Procedure:

1. Determine where on the rack to mount the comparator and mark the location. The brackets are useful in making this determination, and the pin on the back of the bracket helps finding the exact location on the rack.
2. Attach the brackets to the sides of the comparator:
   a. Use M6x1x13 machine screws with captive washer (zinc plated).
   b. Screw one bracket into the clinch nuts on the side of the comparator chassis.
   c. Screw the second bracket into the clinch nuts on the other side of the comparator chassis.
3. Lift the comparator into place on the rack using the pins on the brackets to properly line up the device.
4. Attach the two brackets to the rack:
   a. For a Motorola Solutions modular rack, use M6x1x10 thread forming screws with a black finish.
   b. For a Motorola Solutions open rack, use 1224x5/8 in. thread forming screws (zinc plated).
   c. For your own rack, use hardware appropriate for the rack.
   d. Attach the brackets to both sides of the rack through the upper back openings on the brackets.
   e. Attach the brackets to the rack on both sides through the lower back openings.
5. In the front, attach the chassis to the brackets:
   a. Screw two M6x1x10 thread forming screws (black finish) through the front holes on one side of the comparator chassis and into the bracket.
   b. Screw two M6x1x10 thread forming screws (black finish) through the front holes on the other side of the comparator chassis and into the bracket.

3.4.4

Grounding

The GCM 8000 Comparator has a double lug with two lock nuts on the rear panel where the ground wire connects to the comparator on one end, and to the rack grounding bar on the other. The rack grounding bar is connected to the internal ground system. To use the grounding lug, you need a length of #6 AWG wire with UL - listed ring lugs on both ends. This wire is shipped with the comparator.

3.4.4.1

Bonding and Grounding General Requirements

When and where to use:
Use this procedure to install a Rack Grounding Bar (RGC) to a cabinet or rack. A cabinet or rack includes an RGB with the capacity to terminate numerous ground wires. Equipment added to the cabinet or rack must be attached to the ground bar using solid or stranded 6 AWG copper wire.

The RGB uses dual-hole lugs to terminate ground wires. The minimum number of dual-hole attachments is system dependent and is specified by your organization. This bar provides electrical continuity between all bonds and ground wire with a current carrying capacity equal to or exceeding that of a 6 AWG copper wire.

Refer to the *Standards and Guidelines for Communication Sites* manual for additional information on proper bonding and ground at a site.

IMPORTANT: This procedure assumes that all telephone lines, antenna cables, and AC or DC power cables are properly grounded and lightning-protected.

Procedure:

1. Take the ground wire already attached to the two grounding lugs at the rear of the GCM 8000 Comparator, and connect the other end to the rack grounding bar.
2. Tighten the ground lock nut to 60 inch-pounds (6.94 newton-meters).

3.4.5
Battery Temperature Sensor Mounting

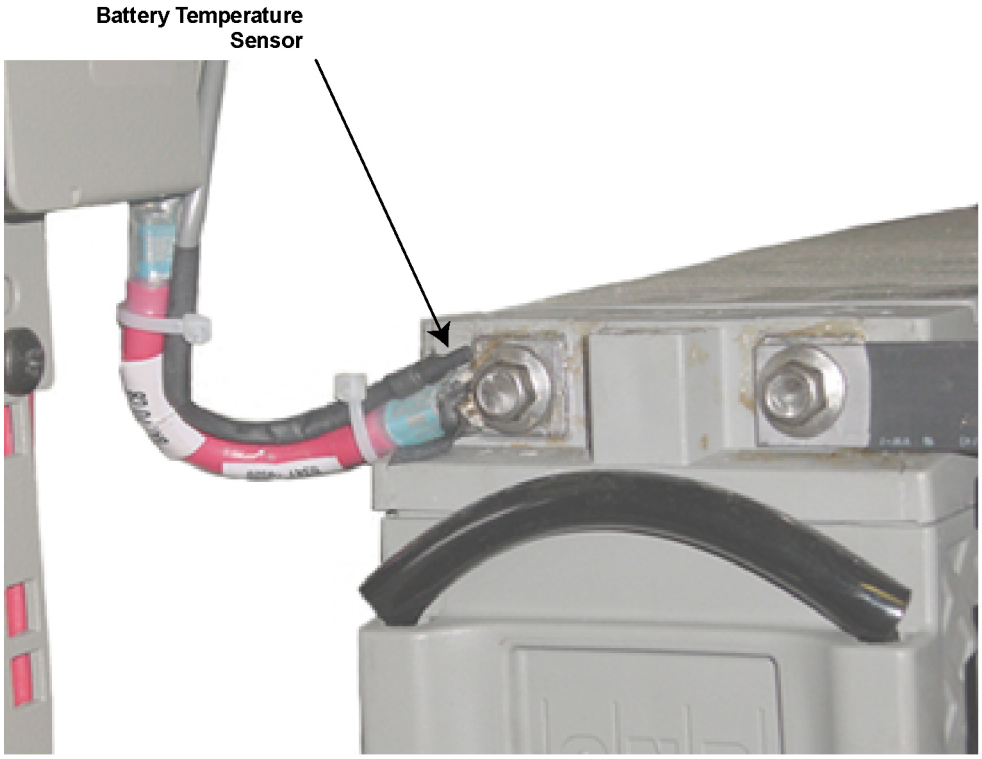
A 40 ft battery temperature sensor cable is shipped with your device. This three-wire cable carries a voltage signal to the power supply from a sensor element which must be mounted close to the storage battery. Voltage is proportional to the battery temperature and the diagnostic circuitry in the power supply module. The 40 ft cable can be extended to a total length of 190 ft using 50 ft extensions (Motorola Solutions part number 3084827Y04. See Motorola Solutions Support Center on page 111.

Mount the sensing element of the temperature sensor so that it detects the actual battery temperature (or the ambient temperature as close as possible to the batteries being charged). The two examples of mounting are as follows:

Example 1

Use cable ties to attach the sensing cable to the positive (or negative) power cable. A minimum of two cable ties should be used (spaced 6 inches apart), with one of the cable ties not more than 2 inches from the sensing element. Mount the sensing element not more than 2 inches from the battery post where the power cable connects. See Figure 10: Battery Temperature Sensor Example 1 on page 55.

Figure 10: Battery Temperature Sensor Example 1



GTR8000_Battery_Temperature_Sensor_1

Example 2

Attach the sensing cable to an existing battery tray support bracket using cable ties or nylon loop straps of the proper size. Mount the sensing element not more than 2 inches from the surface of the batteries being monitored. Use a minimum of two cable ties and/or loop straps to secure the sensing cable to the bracket. Place the cable ties/ loop straps no more than 6 inches apart with one placed no more than 2 inches from the sensing element. See Figure 11: Battery Temperature Sensor Example 2 on page 56.

Figure 11: Battery Temperature Sensor Example 2

3.4.6

GCM 8000 Comparator Front Ports

Figure 12: Front Ports - GCM 8000 Comparator

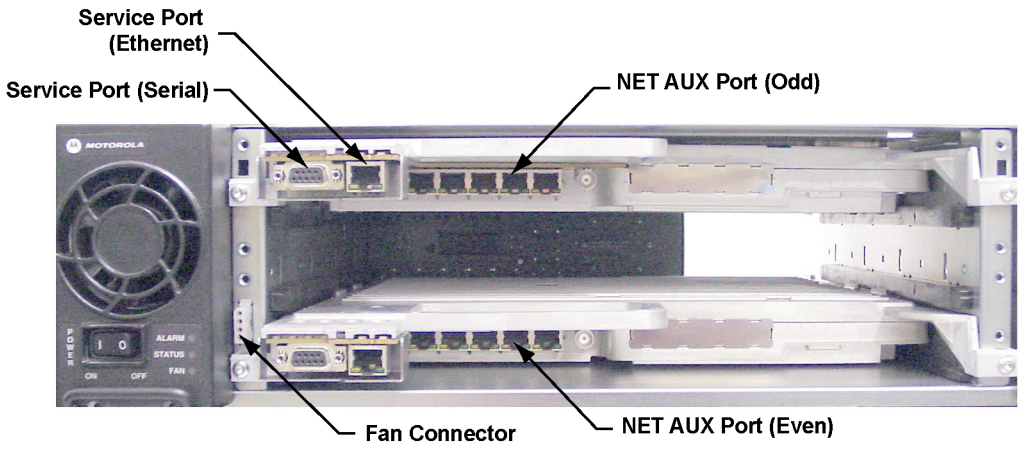


Table 7: Front Ports - GCM 8000 Comparator

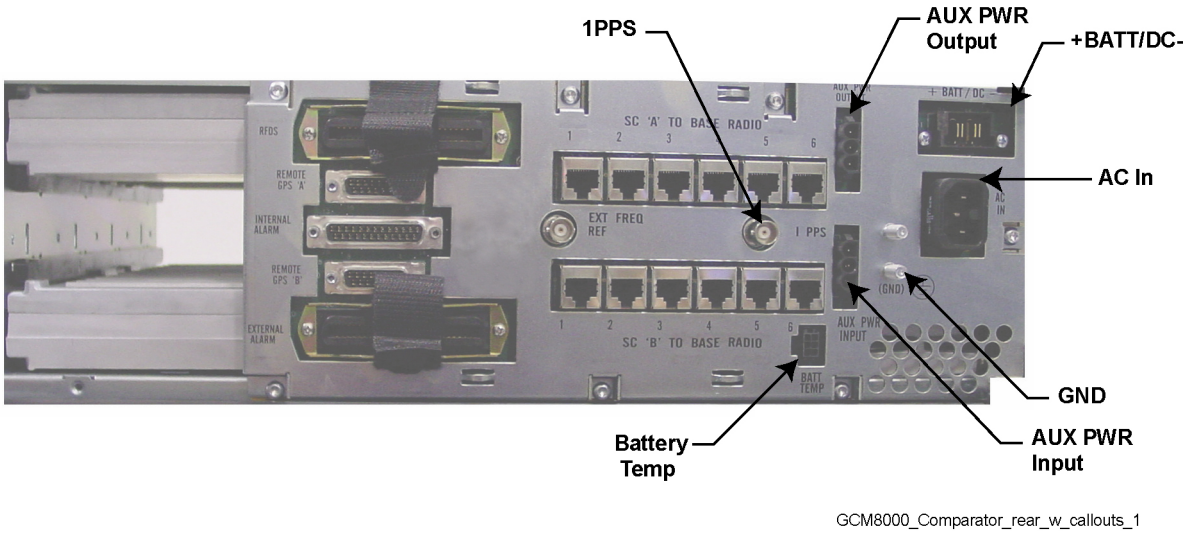
Port/Type	Description
Service Port (Serial)	Service port for initial configuration of the comparator IP address.
Service Port (Ethernet)	Not Used.
NET AUX (Odd)	The port used to connect to Ethernet LAN Switch 1. The Ethernet LAN switch connects to the SDM RTU for local fault monitoring.
NET AUX (Even)	The port used to connect to Ethernet LAN Switch 2. The Ethernet LAN switch connects to the SDM RTU for local fault monitoring.
Fan Connector	Plug in connection when the fan assembly is mounted.

NOTICE: Redundant comparators should not be housed in the same chassis. The redundant comparators must be on separate LAN switches.

For information on Ethernet LAN switch cabling for the preferred control channel comparator, see Chapter 2, “Preferred Control Channel Comparator and Ethernet LAN Switch Configuration” in the *Trunked IP Simulcast Subsystem Prime Site* manual.

3.4.7
GCM 8000 Comparator Rear Ports

Figure 13: Rear Ports - GCM 8000 Comparator



GCM8000_Comparator_rear_w_callouts_1

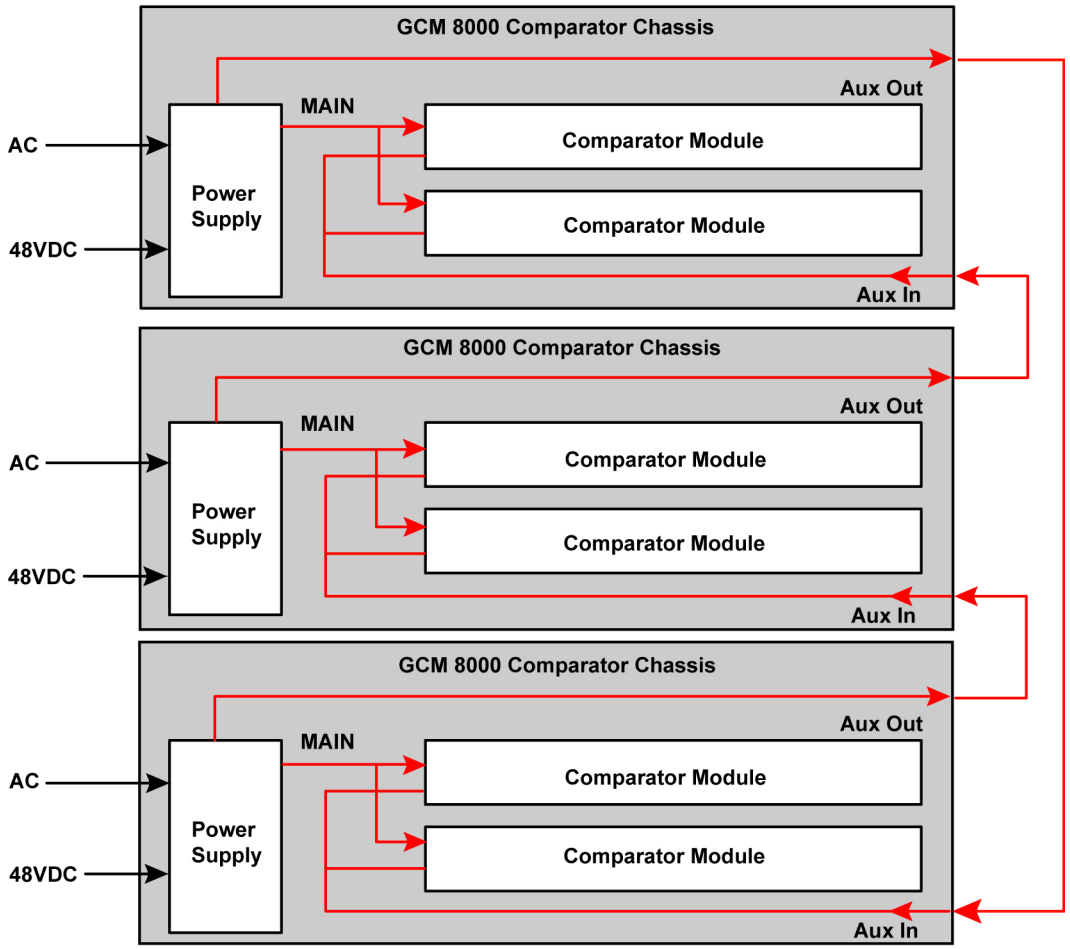
Table 8: Rear Ports - GCM 8000 Comparator

Port	Description
1PPS	For simulcast operation, connection between the TRAK 9100 Simulcast Site Subsystem (SSR) and comparator for time reference. The 1PPS input must have a BNC "T" connected to it. A 50 Ohm termination is on one leg of the "T" and the cable to TRAK 9100 SSR is on the other side of the "T".
AUX PWR Output	The auxiliary output can be connected to another comparator chassis AUX PWR Input to provide a secondary/redundant power source to the other comparator chassis.
+ Batt/DC –	Input from and output to a 48 VDC power supply or backup battery. When AC power is not available, the device switches to operate from a DC source if the optional DC power (8AWG; length 9 ft), CA01400AA is ordered and installed. One end connects into the Batt/DC port and the other end connects into the DC source. The contacts are 39-83503N02 (AMP #53880-2), the receptacle housings are 15-83502N01 (AMP #53884-1) and the mounting ears are 07-83504N01 (AMP #53887-1). 3084869Y06 cable is used for a positive ground system. 3084869Y02 cable is used for a negative ground system.
AC In	Input from 90/264 VAC nominal power source.
GND	Two grounding lugs and cable.
AUX PWR Input	The auxiliary input is connected to another comparator chassis AUX PWR Output as a secondary power source.
	Conventional comparator to a conventional base radio AUX PWR Output.
Battery Temp	Connection to temperature sensor, allowing for temperature compensated battery charging.

NOTICE: The 1PPS input on the rear of the comparator is high impedance. An external termination is needed to properly terminate the cable connected to the input. It is recommended that a BNC “T” and a 50 Ohm BNC termination be connected to the input to terminate the cable.

Figure 14: GCM 8000 Comparator Auxiliary Power Wiring on page 59 shows the cable connections using redundant power via the AUX PWR Input and AUX PWR Output ports between the comparators using a daisy chain for 2, 3 or 4 chassis. All connections must be within the same rack.

Figure 14: GCM 8000 Comparator Auxiliary Power Wiring



GCM 8000 Comparator Aux Wiring

3.5 Installing Device Software Prerequisites

When and where to use: The following tasks are required before you can complete the device software installation and begin the configuration procedures in the “Configuration” chapter.

Process:

1. Transfer and install new software to a device using the Software Download Manager. See Software Download Manager on page 61.
2. Obtain the ASTRO® 25 media. Specifically, you need the Motorola Solutions Device OS Image media. See Loading Device OS Images to the UNC on page 64.

3 Obtain user names, passwords, and procedures required to access the devices on the network. For specific user names and passwords to access devices on the network, contact your system administrator.

4 Set up the users in the IT Admin group in Active Directory Users and Computers. See the *Authentication Services* manual.

5 Obtain the following values from the system administrator:

- Line interface number
- Zone Controller (ZC) site link path 1 IP address
- ZC site link path 2 IP address
- Host name to access the Unified Network Configurator (UNC) server application using Secure SHell (SSH) (**<*username*>** @IP address format)
- Site ID number
- IP address 1 and 2
- Primary and secondary NTP IP addresses

  NOTICE: The following are applicable to systems with Authentication, Authorization, and Accounting (AAA) Servers, Domain Controllers, or Syslog Servers.
- Primary, secondary, and tertiary Domain Name Services (DNS) IP addresses
- Requested DNS Domain Name
- Requested DNS Host Name
- System Name
- Primary SYSLOG Service Name Fully Qualified Domain Name (FQDN)
- Backup SYSLOG Service Name Fully Qualified Domain Name (FQDN)
- Remote Authentication Dial-In User Service (RADIUS) FQDN parameter value
- RADIUS Row Status parameter value
- RADIUS Service Time Out (seconds) parameter value
- RADIUS Service Retransmits Attempts parameter value
- RADIUS Service Dead Timer (min) parameter value
- RADIUS Specific Key parameter value
- RADIUS Service Global Key parameter value

6 Obtain the default credentials (local accounts, central authentication, and SNMPv3) for the device being installed, as well as the updated passwords for those types of accounts (so that you can change the password after you install the device). Contact your system administrator, if you do not have this information. See the *SNMPv3* manual or see Local Password and SNMPv3 Passphrase Troubleshooting on page 109 for more information.

7 Configure the device as a RADIUS client on the RADIUS server. When these devices are configured with a RADIUS key that matches a shared secret for that device in Microsoft Windows Internet Authentication Service (IAS), they become RADIUS clients. They do not join the Active Directory domain. See the *Authentication Services* manual for more information.

8 **NOTICE:** This step is applicable to systems with AAA Servers, Domain Controllers, or Syslog Servers.

To use the VoyenceControl component of the Motorola Solutions centralized configuration application for any of the site device procedures, set up the UNC. Depending on your organizational policies, you may also need to implement a secure protocol between the UNC

and the site device. Before performing any procedures using VoyenceControl, the device must be discovered in VoyenceControl, and the device configurations must be recently pulled to the UNC database. See the following ASTRO® 25 system documentation: *Unified Network Configurator* manual and *Securing Protocols with SSH* manual.

3.6

Software Download Manager

The Software Download Manager (SWDL) is an application that can transfer only, install only, or transfer and install new software to devices. The new software can be installed either locally at a site or on the Network Management subsystem. Individual devices not connected to the system can be downloaded using single device mode.

NOTICE: Throughout this manual, the name SWDL is used to refer to the Software Download Manager application.

Software Download Security Transfer Modes

A software download can be performed using the following security transfer modes:

Clear SWDL
Transfers the software without security, based on the File-Transfer Protocol (FTP)

Secure SWDL
Transfers the software as encrypted, based on the Secure File-Transfer Protocol (SFTP)

NOTICE: All secure sequential and simultaneous transfers use the Diffie-Hellman group exchange. The Diffie-Hellman group exchange is used for devices supporting Diffie-Hellman group exchange. The Diffie-Hellman group exchange enhances the security of Secure Shell (SSH) protocol initial key exchange. See the *Software Download Manager* manual for details.

Before initiating transfer, SWDL connects to the site in the zone to discover all devices. The transfer mode of all devices is displayed in the SWDL window. It is important that all devices have the same SWDL transfer mode. Otherwise, SWDL flags a mismatch of the SWDL transfer modes across site devices.

SWDL provisions the credentials for Secure SWDL as part of initiating the SWDL operation. No user intervention is required. For a single device, Secure or Clear SWDL is configured based on the SWDL Transfer Mode configuration within the Configuration/Service Software (CSS). The Unified Network Configurator (UNC) can be used to schedule and configure all devices in the system at once.

For information on how to configure the secure or clear SWDL transfer mode, see the *Unified Network Configurator* manual and “Configuring Devices for Security” in the *CSS Online Help*.

Software Download Transfer Methods

A software download can be accomplished in two ways:

Site Software Download
Allows you to transfer and install application software from any location within a network. The Software Download Manager resides on the Network Management Client computer and a service computer/laptop loaded with the CSS application. From either of the computers, you can select device types to download software. Site Software Download allows you to select the zone, site, device types, and software download operation to perform. When performing a site software download, the site controller coordinates the software transfer for all trunked base radios, receivers, comparators, and reference distribution modules installed at the site. A site software download can only be performed on a trunked ASTRO® 25 system.

NOTICE: Trunked GPW 8000 Receivers in a circuit simulcast configuration are not supported using a site software download.

Single Device Software Download

Allows you to transfer and install software to a single instance of a device (such as one base radio). This feature gives the technician the ability to install different versions of software. Single device software download is done from a service computer/laptop loaded with the CSS application either connected directly to the device or connected to the network.

NOTICE: Conventional devices and 3600 base radios are supported only in single device software download.

Site Software Download Functionality

When SWDL is connected from a central remote location, SWDL performs a site software download to the site controllers, then to the comparators and base radios or receivers installed at the site. Both active and standby site controller modules have two flash memory banks for storing software. The device application is run from RAM, and is loaded from the active flash memory bank after a reset. One bank is active while the other bank is inactive. The transfer of the software using SWDL is a background process, without interruption of services at the site, that loads the software into the inactive bank. The site controller executes the software from one bank, while software is simultaneously downloaded to the inactive bank. The transfer and install are done in the background. An install causes the site controller to reset and load the RAM from the bank that was installed with the new software.

NOTICE: For geographically redundant prime sites, a site software download should not be attempted while the third Site Controller (SC3) is in the active state.

SWDL communicates with the site controllers to determine the number of existing remote sites and the number of channels. SWDL considers a channel or remote site to be accessible if its status is “Not Unconfigured.” This term means that the site must be set up with a service computer/laptop with CSS or a network management client before software download is performed on the site.

The system downloads software to the site controllers, comparators, base radios, or receivers as a unit. Use SWDL to transfer software to each device type, then perform an install operation. During the transfer, the operation designates a proxy for each device type at each LAN. Site controllers proxy for comparators, and base radios or receivers proxy for each other. The proxy cross-transfers the software to other devices on the LAN. Using proxies minimizes system downtime. Transfers to the LAN are done simultaneously except for the site controller and comparators.

Software installation is done on a channel-by-channel basis, starting with the highest number channel. When a channel software download occurs, the base radio or receiver which incorporates that channel is processed along with the comparator for that channel. For example, if channel 3 was being downloaded, comparator 3 and the base radios or receivers for channel 3 at each of the remote sites would be installed simultaneously.

SWDL operation can be fault managed through Unified Event Manager (UEM), syslog, local SWDL log files, user messages, and device reports.

For further information on SWDL, see the *Software Download Manager* manual.

The operating software can also be loaded using the UNC. See the *Unified Network Configurator* manual to perform single device software downloads (ruthless download) to the devices.

See the *G-Series Equipment System Release User Guide* for SWDL instructions specific to the operating characteristics of your existing system release.

3.7 Installing Devices in the UNC

When and where to use: The Unified Network Configurator (UNC) is the Network Manager used to discover a device and load Operating System images. This process lists the basic steps involved using the UNC on a device.

NOTICE: The UNC is not applicable for K core or non-networked sites.

Process:

1. Discover the device in the UNC. See Discovering a Device in the UNC on page 63.
2. Log in to the UNC server application using PuTTY. See the *Securing Protocols with SSH* manual.
3. Load the operating system images to the UNC. See Loading Device OS Images to the UNC on page 64.
4. Enable FTP services on the UNC. See Enabling FTP Service on page 65.
5. Transfer and install the OS image to the device. See Transferring and Installing the OS Image on page 66.
6. Inspect the device properties for the transferred and installed software. See Inspecting Device Properties for Transferred and Installed Software on page 68.
7. Disable FTP services for the UNC. See Disabling FTP Service on page 69.

3.7.1
Discovering a Device in the UNC

When and where to use:
The discovery process allows the Unified Network Configurator (UNC) to manage the site devices. Once the device is installed, configured through the Configuration/Service Software (CSS), and security parameters are enabled, follow this procedure to discover the device. The configuration information can then be updated using this configuration management application.

The UNC network management solution consists of two applications. Both the UNC Wizard and the VoyenceControl applications are used in this procedure.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Once the device is discovered in the UNC, the OS images and CSS configuration files can be loaded to add a device to a site, which then connects the site to the current ASTRO® 25 zone core.

Procedure:

1. Ensure that Domain Name Services (DNS) is functional on your system. DNS is supplied by a specific server application, which must be operational before you can discover the device.
2. Log on to the UNC Wizard from the Network Management (NM) client, by double-clicking the **Internet Explorer** icon on the desktop.

   The Internet Explorer browser opens.
3. In the **Address** field, enter: `http://ucs-unc0<Y>.ucs:9443/UNCW`

   where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

   The UNC Wizard launches and a login dialog box appears.
4. Type the administrative user name and password. Click **OK**.

   The UNC Wizard appears.
5. From the list of available wizards on the left side, select **Subnet Discovery**.

   The right side of the window is updated with the **Subnet Discovery** form.

6 Select **RF Site** by clicking the **Discovery Type** drop-down list.

7 Enter the **Zone ID** and the **Site ID**. Click **Submit**.

An auto-discovery job is created in the UNC Schedule Manager.

8 Log on to the UNC from the NM client by entering:

`http://ucs-unc0<Y>.ucs`

where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

The UNC client launches and a login dialog box appears.

9 Type the administrative user name and password. Click **OK**.

VoyenceControl launches.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

10 Press F7 (Schedule Manager).

The **Schedule Manager** window appears in the UNC with the discovery jobs.

11 Verify that the **Zone** and **Site** containers include any devices discovered.

IMPORTANT: No site devices should be in the **Lost and Found** folder. If any devices are in the folder, see the *Unified Network Configurator* manual for troubleshooting guidance.

12 In the UNC Wizard, verify the devices by selecting **Channel** under **RF Site Level Configuration**. If multiple zones exist, choose **Zone**.

The device sites are listed, which means they are available for channel configuration.

3.7.2
Loading Device OS Images to the UNC

Prerequisites: This procedure requires the Motorola Solutions device Operating System (OS) Image media. Locate the Transport OS Image media packaged with the Network Management media.

When and where to use: This procedure loads the OS images for the devices for distribution through the Unified Network Configurator (UNC). Once OS images are distributed to the UNC, you can update the device Configuration/Service Software (CSS) configuration files to the UNC.

Procedure:

1 Launch a Secure SHell (SSH) terminal server session in PuTTY to access the UNC **Server Administration** menu. See the *Securing Protocols with SSH* manual.

2 From the UNC **Server Administration** menu, select **OS Images Administration**. Press ENTER.

3 From the OS **Images Administration** menu, select **Load new OS images**. Press ENTER.

A message appears indicating there are two methods for loading OS Images.

4 Insert the **Motorola Solutions Device OS Images** media into the CD/DVD-ROM drive of the server.

The drive light starts blinking on the server.

5 When the drive light stops blinking, press ENTER.

The OS images load on the UNC.

6 From the menu, select **View OS Images**. Press ENTER.

The device software image appears.

7 From the menu, select **Eject CD**. Press ENTER.

The media ejects from the drive on the server.

8 Remove the **Motorola Solutions Device OS Images** media from the CD/DVD-ROM drive of the server.

9 To log out of the server, press ENTER.

The **User Configuration Server Administration** menu appears.

10 Press ENTER again.

The prompt appears.

3.7.3
Loading Software to a Device

NOTICE: These procedures are for a single device download. For a site download, see Software Download Manager on page 61.

The following procedures describe how to load software images onto Unified Network Configurator (UNC) and download and install this software to the device. Secure protocols for software download is the preferred approach to transfer operations. However, as a backup option, FTP service can be enabled before installing the software.

3.7.3.1
Enabling FTP Service

When and where to use: Follow this procedure to enable FTP service before installing the OS software.

Procedure:

1 Launch a Secure Shell (SSH) terminal server session in PuTTY to access the Unified Network Configurator (UNC) **Server Administration** menu. See the *Securing Protocols with SSH* manual.

2 From the Server Administration menu, select **Unix Administration**. Press ENTER.

3 From the Unix Administration menu, select **FTP Services**. Press ENTER.

4 From the FTP Services menu, select **Enable FTP service**. Press ENTER.

The FTP Services are enabled and available for software transfer and install operations.

3.7.3.2
Transferring and Installing the OS Image

When and where to use: Use this procedure to download the OS from the Unified Network Configurator (UNC) to the device.

Procedure:

1. On the Private Network Management (PNM) client where you set up VoyenceControl, double-click the UNC shortcut on the desktop.

   You can also paste the following address into an IE web browser: `http://ucs-unc0<Y>.ucs`, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

   Internet Explorer opens to the URL of the application server, and a VoyenceControl client session launches with the welcome page.

   Figure 15: VoyenceControl Welcome Page

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

2. Click the **launch VoyenceControl™** link.

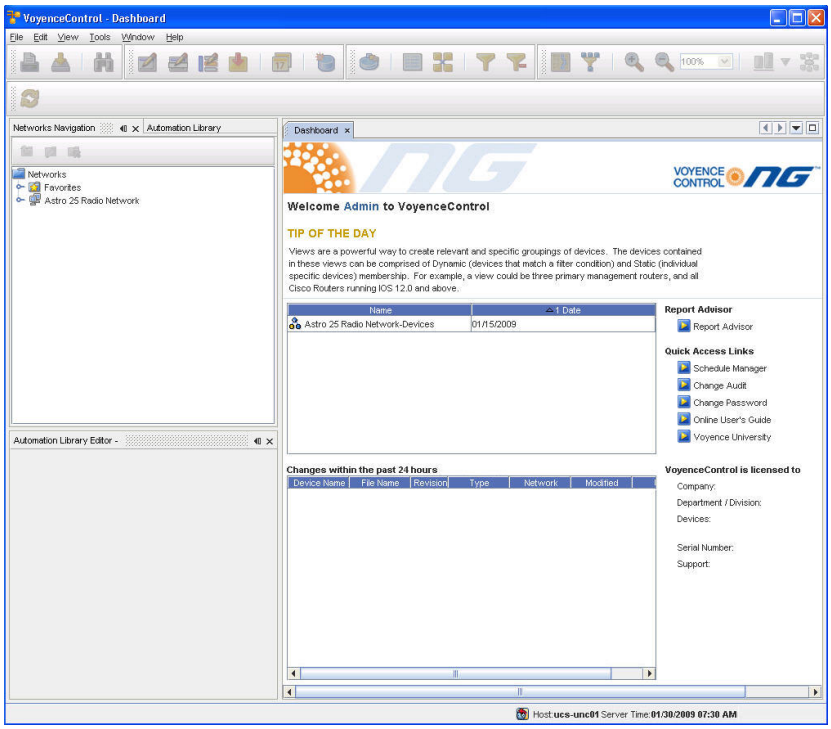
   A VoyenceControl client session launches with the login window.

   Figure 16: VoyenceControl Login Window

3 Enter the User ID and Password. Click **OK**.

The **VoyenceControl Dashboard** appears.

Figure 17: VoyenceControl Dashboard



4 In the left navigation pane, expand **Networks**, then select **ASTRO 25 Radio Network**, then **Views**.

The list of options expands.

5 From the navigation pane, double-click **Motorola <device>**.

The view opens and all currently discovered devices appear.

6 From the menu, select **Tools** → **OS Inventory**.

A list of the OS images appears.

7 Verify OS images loaded on the UNC server appear in the OS inventory.

NOTICE: These images were automatically created during the Loading Device OS Images to the UNC on page 64 procedure.

8 Under **Networks** in the navigation pane, select one or more devices from the same device class by right-clicking the selections.

9 From the menu, select **Update OS Image**.

10 From the **Select OS Image** window, select **Software Image**. Click **Next**.

11 From the **Update OS Image** window, select each device that appears in the **Selected Devices** section.

This action associates a version to a device instance.

NOTICE: In most cases, the “summary of device partitions” is already set up and the values in step 11 through step 14 must be verified.

12 Select **nvm partition** from the **Manage Partition for Device** section.

NOTICE: Selecting **nvm partition** defines where the OS image is transferred and is the only choice for the device.

13 From the **Selected Image** section, select the image for this device.

NOTICE: Ignore the **Install** and **Copy** check boxes.

The **Image Info** tab is populated and informs the application which image to use.

14 Click **Add**.

The **Summary of Device Partitions for Device** populates and confirms the proper setup.

15 Select the **Device Options** section, **Software Operations**, then choose **transfer**, **install**, or **both**.

These selections indicate which operations occur when the job is executed.

NOTICE: If **transfer** is chosen, select the install option later to complete the installation. If **both** is chosen, the software is transferred and installed. There are up to two resets of the device during installation.

16 Click **Schedule**.

17 From the **Schedule Push Job** window, configure the schedule information. Click **Approve and Submit**.

The job is approved and can be viewed in the **Schedule Manager** window.

NOTICE: If only **Submit** is chosen, the job must be approved later.

18 Verify the job status by pressing F7 (Schedule Manager).

The **Schedule Manager** window appears in the UNC with the discovery jobs.

3.7.3.3
Inspecting Device Properties for Transferred and Installed Software

When and where to use: When the software has been transferred and installed, follow this procedure to inspect the device properties before assuming the installation was a success and disabling FTP service

Procedure:

1 From the **Device** view, right-click the device, select **Pull**, and then **Pull Hardware Spec**.

The current software version information is updated in the Unified Network Configurator (UNC).

NOTICE: Skip this step if a Pull All or Pull Hardware Spec has already occurred.

2 From the **Device** view, right-click on the device, and then choose **Properties**.

The **Device Properties** window appears.

NOTICE: Select the **Properties** icon to view the device properties appear directly within the **Device** view.

3 Choose the **Configuration** tab, and then the **Hardware** tab.

4 Double-click the **Chassis** object from the **Physical Hardware** properties.

5 From the **Chassis** property tree, view the following properties and their values:

- **Bnk1:<*device*>**: Transferred software in bank 1.
- **Bnk2:<*device*>**: Transferred software in bank 2.
- **<*device*>**: Installed and Running Software.

NOTICE: The Table format can be used (instead of the Diagram format) to view the Installed and Running Software in the **Device** view.

3.7.3.4 Disabling FTP Service

When and where to use: Follow this procedure to disable the FTP service after the transfer and installation of the software is completed.

Procedure:

1 Launch a Secure SHell (SSH) terminal server session in PuTTY to access the Unified Network Configurator (UNC) **UNC Server Administration** menu. See the *Securing Protocols with SSH* manual.

2 From the **UNC Server Administration** menu, select **Unix Administration**. Press ENTER.

3 From the Unix Administration menu, select **FTP Services**. Press ENTER.

4 From the **FTP Services** menu, select **Disable FTP service**. Press ENTER.

The FTP services are disabled and unavailable for software transfer and install operations.

5 To back out of the menus, press Q three times.

6 At the prompt, enter: `exit` to return to the previous menu.

7 To log out of the application, enter: `exit`.

8 Close the PuTTY connection.

This page intentionally left blank.

Chapter 4

GCM 8000 Comparator Configuration

This chapter details configuration procedures relating to the GCM 8000 Comparator.

4.1 Configuration Software

Configuration of a device can be done on two software applications: Configuration/Service Software (CSS) and Unified Network Configurator (UNC).

CSS
is used to configure the parameters on the device. CSS can access devices remotely over the network, or locally through an Ethernet/serial connection to the service port on the device or through a LAN switch. CSS also can be used to view status information, equalize batteries, and check internal logs of the equipment at the site. See the *CSS Online Help* for configuration details.

UNC Wizard
is a component of UNC used to configure the parameters of a site, subsite, and channel. See the *UNC Wizard Online Help* for configuration details.

VoyenceControl
is a component of UNC used to pull and push configurations and configure the parameters of the device. See the *Unified Network Configurator* manual for general information about using VoyenceControl functions.

NOTICE: While it is possible to configure a conventional device using the UNC, it is preferable to use CSS because configuration dependencies are enforced.
The UNC is not applicable for K core or non-networked sites.

All parameters are programmed locally when the site is installed but not linked to a network. Test all parameters before making the site available. The ability to locally program provides the means to test the site before making it available for system operation.

4.2 Discovering a Device in the UNC

When and where to use: Use these high-level steps to discover the devices in the Unified Network Configurator (UNC). See the *Unified Network Configurator* manual for details on discovering devices.

Process:

1. Use the UNC Discovery Wizard to:
   - Discover the devices.
   - Upload configurations for the devices.
   - Generate changes for non-compliant devices.
2. Approve jobs (if any).

4.3 Default Speed/Duplex Settings

The GCM 8000 Comparator modules are configured for auto-negotiation and use auto-negotiation with the site switch to set the speed and duplex values for the 100BaseT Ethernet port. In typical operation the auto-negotiation with the site switch results in the speed being set to “100 Mbps” and the duplex set to “Full.”

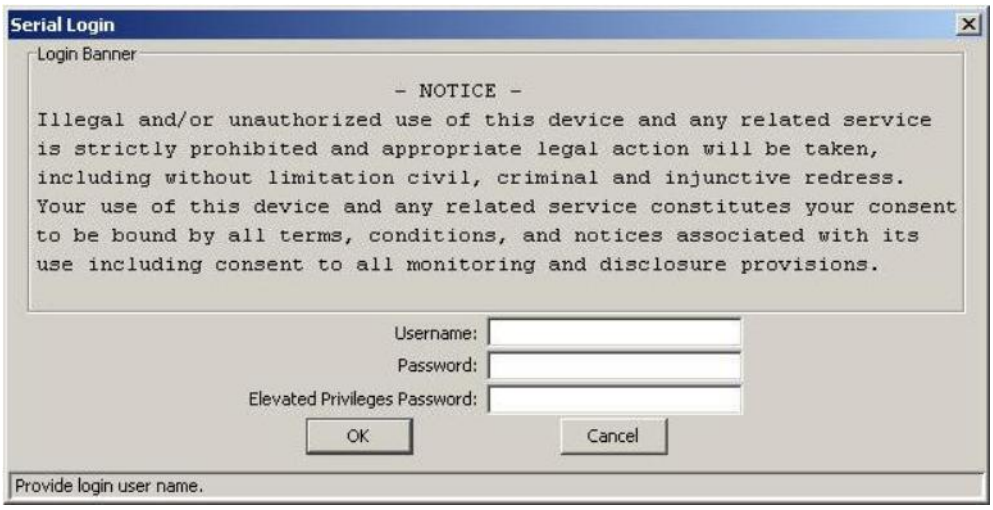
4.4 Security/Authentication Services

If the device supports SNMPv3 protocol, a pop-up dialog box appears displaying the SNMPv3 Password Prompt when logging in to a device through Configuration/Service Software (CSS) using an Ethernet connection. For configuration details, see the *Information Assurance Features Overview*, *Software Download Manager*, and *SNMPv3* manuals. See Figure 18: SNMPv3 Security Level Option Prompt on page 72.

Figure 18: SNMPv3 Security Level Option Prompt

A pop-up window appears displaying the File Transfer Access Services for CSS. Use this logon when communicating to a device through CSS using either an Ethernet or DB-9 Serial Port connection. See Figure 19: CSS Login Banner on page 73.

Figure 19: CSS Login Banner



4.5 Device Configuration in CSS

This section covers configuration of a device using the Configuration/Service Software (CSS).

NOTICE: The IP address for the device is available through a serial port connection in the **Tools** → **Set IP Address** from the CSS menu.

4.5.1 Initial Configuration of a Device in CSS

When and where to use: Use this process to initially configure the device in CSS.

Process:

1. Perform the following configuration steps that require a serial connection. See Connecting Through a Serial Port Link on page 74.
   - **a** Set the IP address and pairing number of the device. See Setting the Device IP Address and Pairing Number in CSS on page 75
   - **b** Set the serial security services. See Setting the Serial Security Services in CSS on page 77.
2. Perform the following configuration steps that require an Ethernet connection. See Connecting Through an Ethernet Port Link on page 78.
   - **a** Set the pairing number of the device. See Setting the BR/CM Pairing Number in CSS on page 81.
   - **b** Set the current date and time. See Setting the Date and Time in CSS on page 82.
   - **c** Change the SNMPv3 configuration and user credentials on a selected device in the site. See Changing SNMPv3 Configuration and User Credentials in CSS on page 82.
   - **d** Create, update, or delete an SNMPv3 user. See Adding or Modifying an SNMPv3 User in CSS on page 85.
   - **e** Verify the SNMPv3 credentials. See Performing an SNMPv3 Connection Verification in CSS on page 85.
   - **f** Configure DNS. See “Configuring DNS in CSS” in the *Authentication Services* manual.

g Set the SWDL transfer mode. See Setting the SWDL Transfer Mode in CSS on page 86

h Configure for SSH. See the *Securing Protocols with SSH* manual, "Configuring SSH for RF Site Devices and VPMs in CSS" section in Chapter 4.

i Enable RADIUS Authentication. See Chapter 7, “Configuring RADIUS Sources and Parameters in CSS” in the *Authentication Services* manual. Make sure that the comparators have been added to the RADIUS servers on the domain controllers as RADIUS clients.

j Enable Centralized Authentication. See Chapter 7, “Enabling/Disabling Centralized Authentication in CSS” in the *Authentication Services* manual.

k Set the Local Cache Size for Centralized Authentication. See Chapter 7, “Setting the Local Cache Size for Central Authentication in CSS” in the *Authentication Services* manual.

l Customize the login banner text (optional). See Customizing the Login Banner in CSS on page 85.

m Enable Centralized Event Logging (if required by your organization). See Chapter 6, “Enabling/Disabling Centralized Event Logging on Devices in CSS” in the *Centralized Event Logging* manual.

3 Set up the local Password Configuration (optional). See Setting the Local Password Configuration in CSS on page 87.

4.5.2
Connecting Through a Serial Port Link

Prerequisites: This procedure assumes that the Configuration/Service Software (CSS) application is loaded on your service computer/laptop. See the *Private Network Management Client* manual.

When and where to use: This procedure describes the steps required to connect through a serial port link to set the IP address of the device and to set the serial security services. Perform all other device function and feature configurations through an Ethernet port connection in the CSS.

Procedure:

1 Connect a serial cable to a service computer/laptop running CSS, and the serial connector on the device module. The serial cable is an RS232, female DB-9 to male DB-9 straight through cable. If the service computer/laptop does not have a serial port, use a USB-to-serial converter external device.

2 Open the CSS application.

3 From the menu, select **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

4 In the **Connection Type** area, select **Serial**.

The **Serial Settings** area on the dialog box becomes enabled.

5 In the **Serial Port** field, select the communication port that matches the one selected on the service computer/laptop.

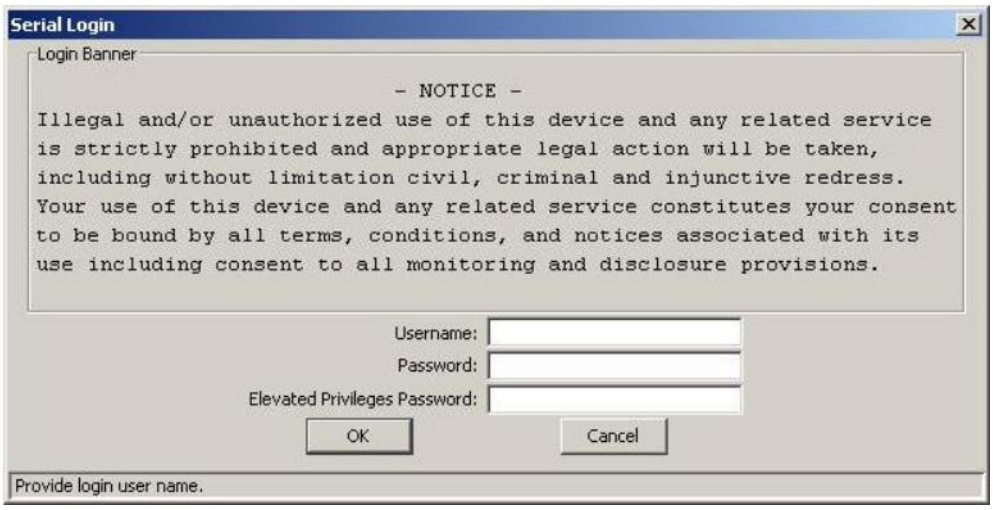
6 In the **Baud Rate** field, select the baud rate with which you want to communicate with the device.

- Baud Rate 19200

7 Click **Connect**.

A login/password prompt screen appears.

Figure 20: CSS Login Banner



8 Provide the required credentials. Perform one of the following actions:

- If a domain controller is available on the network, enter the **Username** and **Password** for the RADIUS service user account assigned to the netwadm group in the Active Directory. (The default service user is `serviceuser`.)
- If a domain controller is not available on the network, enter the **Username** and **Password** for the local bts_service account.
- If the **Elevated Privileges Password** field is active, enter the **Elevated Privileges Password** that was set up for this device.

When accessing the device, if the default passwords do not work, the passwords may have been set to default values by a different system release of software. See "Resetting Device Passwords" in the *CSS Online Help* to reset the passwords to the current software release defaults. If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the [**Username**, **Password**, and **Elevated Privileges Password**] fields, as they cannot be left blank.

9 To access the device and close the dialog box, click **OK**.

The blank CSS main window appears.

NOTICE: The **Service** menu is not available until you read the configuration file from the device using an Ethernet connection.

4.5.3
Serial Connection Configurations

The following procedures set configuration parameters in the Configuration/Service Software (CSS) using a serial connection.

4.5.3.1
Setting the Device IP Address and Pairing Number in CSS

Prerequisites: Obtain the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, access to

the device or to the user credentials is denied. See Local Password and SNMPv3 Passphrase Troubleshooting on page 109.

NOTICE: Setting or changing the device IP Address causes the SNMPv3 configuration and user credentials to automatically reset.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through a serial port link. See Connecting Through a Serial Port Link on page 74.
2. From the menu, select **Tools** → **Set IP Address/BR_CM Pairing Number**.

   NOTICE: If the device is not in a voting or simulcast IP only topology, the menu item is shown as **Set IP Address/Box Number**.

   The **Set IP Address and Base Radio/Comparator Pairing Number** dialog box appears or the **Set IP Address and Box Number** dialog box appears.
3. In the **Device IP Address** field, enter the device IP address. Click **Set Device IP Address**.
4. In a voting or simulcast IP only topology, enter the device pairing number. Click **Set BR/CM Pairing Number**.
5. Click **OK** to close the dialog box.
6. Click **Reset** to initiate a hardware restart.

   SNMPv3 user credentials reset to their factory default values.
7. Click **Close** to close the dialog box.
8. To reconfigure the SNMPv3 user credentials, see Changing SNMPv3 Configuration and User Credentials in CSS on page 82.

4.5.3.2
Pairing To a Base Radio/Receiver

When operating in a voting, multicast, or simulcast IP configuration, comparators must be paired to base radios/receivers using the BR_CM Pairing Number. The BR_CM Pairing Number for both the base radio/receiver and comparator is used to create an IP multicast group that allows the base radio/receiver and comparator to talk to each other. The base radio/receiver listens for messages that the comparator sends in order to establish an IP connection with all the paired base radios/receivers. When the base radio/receiver receives the message from the comparator, it extracts the comparator's IP address from the message and uses it to send received voice and data back to the comparator.

Communication from the comparator to the paired base radios/receivers always uses a multicast IP address. Communication between the paired base radios/receivers to the comparator always uses a unicast IP address.

The multicast IP address is calculated based on the base radio/receiver and comparator pairing number and the formula as follows:

For Conventional Systems:

224.10.100.nnn, where nnn is: (2 * channel number) - 1 for channel number between [1, 127]
224.10.101.nnn, where nnn is: (2 * (channel number – 127) - 1) for channel number between [128, 200]

For Trunking Multi Site Systems:

224.100.102.nnn, where nnn is: 100 + (2 * channel number) - 1

NOTICE: The Base Radio/Comparator Pairing number is not used for Circuit (V.24 or V.24 hybrid link) configurations.

See Setting the Device IP Address and Pairing Number in CSS on page 75 on how to set the Pairing Number. Setting the pairing number can also be performed using an Ethernet connection. See Setting the BR/CM Pairing Number in CSS on page 81.

4.5.3.3
Serial Security Services in CSS

The Serial Security Services in Configuration/Service Software (CSS) enables the secure services and changes the device password.

NOTICE: The Serial Security Services must be set before changing the SNMPv3 configuration and user credentials on a selected device in the site.

Before enabling this parameter, any login and password may be used on the File Transfer Access Services login window to access a device. After Authentication Services are enabled, the login and password provided is checked against the following authentication sources:

Stored password
RF site devices support a configurable password for the Local Service and Elevated Privileges accounts. The password is verified against the stored password for these accounts.

Built-in logins and passwords
RF site devices support built-in login/password combinations for a login by services such as the software downloads. Only certain software download login names are authenticated in this way.

Centralized Authentication
For authentication through centralized accounts instead of Local Service, Elevated Privileges, and built-in user accounts, use the **Configure the Centralized Authentication** parameter in CSS for the Challenge Handshake Authentication Protocol (CHAP). See “Enabling/Disabling Centralized Authentication with CSS” in the *Authentication Services* manual. This procedure requires an Ethernet connection to the device being configured.

4.5.3.3.1
Setting the Serial Security Services in CSS

Prerequisites: Obtain the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. See Local Password and SNMPv3 Passphrase Troubleshooting on page 109. Changing to the incorrect user credentials may lead to not being able to access the device through Configuration/Service Software (CSS) or Secure Shell (SSH).

Procedure:

1. Connect to the device using CSS through a serial port link. See Connecting Through a Serial Port Link on page 74.
2. From the menu, select **Security** → **Device Security Configuration** → **Security Services (Serial)**.
3. From the **Security Services Configuration** dialog box, set the **Test Application Configuration** field according to your organizational policies. The recommended secure configuration is **Disabled**.
4. Set the **Authentication Services** field to **Enabled**. Click **Apply**.

   This field enables local authentication services and must be enabled as a prerequisite for centralized authentication.
5. Set the **Password Reset Mechanism** field.

   This field allows a reset of the passwords for two built-in device accounts to their default values.

6 To update the password for the device, select either **Service Account** or **Elevated Privilege** from the drop-down list. Click **Update password**.

7 In the **Change Account Password** dialog box, enter the old password, then enter a new password, and confirm the new password before clicking **Change Password**.

8 To save the new password, click **OK**.

The **Change Account Password** dialog box closes.

4.5.3.4
Resetting SNMPv3 User Credentials to Factory Defaults in CSS

Prerequisites: Obtain the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. To obtain the keys for resetting either password or SNMPv3 passphrases for the device, contact Motorola Solutions Support Center (SSC). Changing to the incorrect user credentials may lead to not being able to access the device through Configuration/Service Software (CSS) or Secure SHell (SSH).

Procedure:

1 Connect to the device using CSS through a serial port link. See Connecting Through a Serial Port Link on page 74.

2 From the menu, select **Security** → **SNMPv3 Configuration** → **Reset SNMPv3 Configuration (Serial)**.

The **Reset SNMPv3 Configuration** dialog box opens.

3 Click **Reset SMPv3 Configuration**.

The SNMPv3 configuration is reset to factory defaults in the device.

4 Click **Exit**.

The **Reset SNMPv3 Configuration** dialog box closes.

5 To reboot the device for the SNMPv3 user credentials to take effect, perform the following actions:

a From the menu, select **Tools** → **Set IP Address/Box Number** or **Set IP Address/BR_CM Pairing Number**.

b In the dialog box, click **Reset**.

The device reboots.

6 Proceed to Changing SNMPv3 Configuration and User Credentials in CSS on page 82.

4.5.4
Connecting Through an Ethernet Port Link

Prerequisites: Load Configuration/Service Software (CSS) on the service computer/laptop. See the *Private Network Management Client* manual if necessary or see the instructions in the CSS DVD jewel box for instructions on loading the CSS onto the service computer/laptop.

When and where to use: Use the Ethernet port link to configure all CSS parameters for the device.

Procedure:

1 Connect a service computer/laptop to a device using one of the following methods:

NOTICE: Normally the service computer/laptop is connected through the local site switch or remotely through the network. Do not connect directly to the Ethernet service port of the device unless downloading software or individually configuring the device.

a **Remote Connection to Network or Local Site Switch:**

1 Connect remotely to the network or to the local site switch using a straight-through an Ethernet straight-through Ethernet cable.

2 If connecting to the local site switch, configure the Ethernet interface of the service computer/laptop to a Speed/Duplex setting of **Auto-Negotiate**. Set the IP address of the service computer/laptop to an unused IP address on the subnet of the local site. The IP address on the subnet varies depending on the site and zone numbers.

b **Direct Connection to Front Ethernet Service Port:**

1 Connect directly to the front panel Ethernet service port with a straight-through Ethernet cable.

2 If connecting to a base radio or receiver, set the IP address of the service computer/laptop to 192.168.x, where x is any number between 2 and 253.

3 If connecting to a site controller or reference distribution module, set the IP address of the service computer/laptop to an unused IP address on the subnet of the local site. The IP address on the subnet varies depending on the site and zone numbers.

4 Configure the Ethernet interface of the service computer/laptop to a Speed/Duplex setting of **Auto-Negotiate**

NOTICE: The comparator does not support a direct connection to the front panel Ethernet service port. The connection must be done remotely through the network or through the local site switch.

2 Open the CSS application.

3 From the menu, select **Tools** → **Connection Configuration**.

4 From the **Connection Screen**, in the **Connection Type** area, select **Ethernet**.

5 If connected directly to the front panel Ethernet service port of a base radio or receiver, click **Front Panel Ethernet** and go to step 7.

6 Perform one of the following actions:

If…	Then…
If you know the IP address for the device,	perform the following actions: **a** In the **Device IP Address** field, enter the IP address for the device. **b** Click **Connect**. **c** Go to step 7.
Trunked Device: If you do not know the IP address, but know the system identification of the device (the zone,	perform the following actions: **a** Click **Device Name Wizard** to open the **Device Name Wizard** dialog box. **b** From the **Device** drop-down list, select the relevant device type.

If…	Then…
physical site, subsite, and device ID of the device),	**c** In the **Zone**, **Physical Site**, **Subsite**, and **Device ID** fields, enter the proper values. **NOTICE:** Some fields, such as **Subsite**, do not allow entries for some devices. Therefore, select the device first. **d** Click **OK**. The Domain Name Services (DNS) information of the device automatically appears in the **Device IP Address** field. **e** Click **Connect**. **f** Go to step 7.
Conventional Device: If you do not know the IP address,	perform the following actions: **a** Establish a serial connection to the device. See Connecting Through a Serial Port Link on page 74. **b** For a base radio, receiver, or comparator, from the menu, select **Tools** → **Set IP Address/BR_CM Pairing Number**. For a site controller or reference distribution module, select **Set IP Address/Box Number**. **c** In the **Device IP Address** field, record the IP address. **d** Re-establish an Ethernet connection and repeat steps 1 through 4. **e** In the **Device IP Address** field, enter the IP address for the device. **f** Go to step 7.

7 To make the connection, click **Connect**.

If this device is SNMPv3-capable, the **SNMPv3 Passphrase Prompt** dialog box appears.

Figure 21: SNMPv3 Passphrase Prompt

8 In the **SNMPv3 Passphrase Prompt** dialog box, enter the **User Information** and **Passphrase Information**. Click **OK**. If Authentication Services are not enabled on a device, click **OK** when the dialog box appears.

9 From the menu, select **File** → **Read Configuration From Device**.

The parameters download from the device to the service computer/laptop. When the download is complete, the CSS main window opens. Use the map on the left side of the screen to view configuration information for the device.

4.5.5
Ethernet Connection Configurations

The following procedures set configuration parameters in the Configuration/Service Software (CSS) using an Ethernet connection.

4.5.5.1
Setting the BR/CM Pairing Number in CSS

When and where to use:
Set the pairing number for the base radio, receiver, and comparator using Configuration/Service Software (CSS) when operating in a voting, multicast, or simulcast IP configuration using an Ethernet connection.

Procedure:

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.

2 From the menu, select **Service** → **BR/CM Pairing Number**.

3 Enter the pairing number. Click **OK**.

The pairing number is set.

4.5.5.2
Setting the Date and Time in CSS

This procedure provides the date and time to the device.

When and where to use: During installation, the date and time is set through an Ethernet cable connected directly to the Ethernet port of the device. After installation, this procedure may be performed remotely.

NOTICE: If a power outage occurs, the device does not retain the date and time settings.

Procedure:

1 Connect to the device using CSS through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.

2 From the menu, select **Tools** → **Set Device Date and Time**.

3 Enter the current date and time. Click **OK**.

The date and time are set.

4.5.5.3
Changing SNMPv3 Configuration and User Credentials in CSS

Prerequisites: Obtain the required SNMPv3 credentials information (Authentication passphrase, Encryption passphrase, and Authoritative Engine ID) to configure the device before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. See Local Password and SNMPv3 Passphrase Troubleshooting on page 109. Changing to the incorrect user credentials may lead to not being able to access the device from the Unified Network Configurator (UNC), or for the device to be unable to send alarms to the Unified Event Manager (UEM) (for fault management).

When and where to use: This procedure changes the SNMPv3 configuration and user credentials from Configuration/Service Software (CSS) on a selected device in the site. For more information on this feature, see the *SNMPv3* manual.

NOTICE: During installation, perform this procedure through an Ethernet cable connected directly to the Ethernet port of the device. After installation, this procedure may be performed remotely from CSS.

Procedure:

1 Connect to the device using CSS through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.

2 From the menu, select **Security** → **SNMPv3 Configuration** → **Configure SNMPv3 Users (Ethernet)**.

The **SNMPv3 Passphrase Prompt** dialog box appears with **MotoAdmin** as the selected SNMPv3 user.

3 In the **SNMPv3 Passphrase Prompt**, enter the appropriate **Authentication** and **Encryption Passphrases** in the text fields.

NOTICE: When accessing the device for the first time, if the default passphrases do not work, the passphrases may have been set to default values by a different system release of software. See “Reset SNMPv3 Configuration (Serial)” in the *CSS Online Help* to reset the passphrases to the current software release defaults.

4 If connecting remotely through the network to a different device, perform one of the following actions. Otherwise, go to step 5.

If…	Then…
If you know the IP address for the device,	perform the following actions: **a** In the **Device IP Address** field, enter the IP address for the device. **b** Go to step 5.
If you do not know the IP address, but know the system identification of the device (the zone, physical site, subsite, and device ID of the device),	perform the following actions: **a** Click **Device Name Wizard**. **b** From the **Device** list box, select the desired device type. **c** In the **Zone**, **Physical Site**, **Subsite**, and **Device ID** fields, enter the proper values. **NOTICE:** Some fields, such as **Subsite**, do not allow entries for some devices. Therefore, select the device first. **d** Click **OK**. The Domain Name Services (DNS) information of the device automatically appears in the **Device IP Address** field. **e** Click **Connect**. **f** Go to step 5.

5 Click **OK**.

If the passphrases are authenticated, the **Configure SNMPv3 Users** window appears. If the connection fails, a message appears.

6 To update the SNMPv3 credentials for a selected user, from the **User Information** section, select a Username in the **Username** drop-down list.

The CSS retrieves the current credentials from the device for a selected user.

NOTICE: Depending on the user selected, some fields on this dialog box become read-only or disabled. Click **Cancel** at any time to discard changes made to a selected user.

7 To change or update the SNMPv3 security level for a selected user, from the **User Information** section, select the security level in the **Security Level** drop-down list.

The security level options are:

NoAuthNoPriv
Neither the **Authentication Passphrase** nor **Encryption Passphrase** are needed for communicating with the device.

AuthNoPriv
Authentication Passphrase is needed; but no **Encryption Passphrase** is needed for communicating with the device.

AuthPriv
Both **Authentication Passphrase** and **Encryption Passphrase** are needed for communicating with the device.

The **User Status** field reflects the current operational status of the selected SNMPv3 User. The **Status Types** include:

Active
User configured on the device; the **Update** and **Delete** options are enabled.

Not in service
User configured on the device; the **Update** and **Delete** options are enabled.

Not ready
User configured on the device; the **Update** and **Delete** options are enabled.

Not present
Not present on the device; the **Create** option is enabled.

The security level of the selected user is set.

8 To change the Authentication Passphrase for the selected SNMPv3 user, if applicable to the selected security level, perform the following actions:

a From the **Authentication Passphrase** section, enter the passphrase into the **Old Passphrase** field.

NOTICE: If you do not know the passphrase, select the **I do not remember old passphrase** check box.

b Enter the new passphrase into the **New Passphrase** field.

NOTICE: The passphrase must be between 8 and 64 characters in length and consist of upper or lowercase alphanumeric characters (excluding the @ # $ ^ or _ characters).

c Enter the same new passphrase into the **Confirm New Passphrase** field.

9 To change the encryption passphrase for the selected SNMPv3 user, if applicable to the selected security level, perform the following actions:

a From the **Encryption Passphrase** section, enter the old passphrase into the **Old Passphrase** field.

NOTICE: If you do not know the passphrase, select the **I do not remember old passphrase** check box.

b Enter the new passphrase into the **New Passphrase** field.

c Enter the same new passphrase into the **Confirm New Passphrase** field.

10 To change the Authoritative Engine Identifier, applicable to MotoInformA and MotorInformB users only, perform the following actions:

a From the **Authoritative Engine ID** section, select the desired current engine ID from the **Current Engine ID** drop-down list.

b In the **New Engine ID** field, enter the new engine ID.

NOTICE: The new engine ID must be between 1 and 27 characters and comply with the Engine ID Domain Name Syntax.

11 To create, update, or delete SNMPv3 users, go to Adding or Modifying an SNMPv3 User in CSS on page 85.

4.5.5.3.1
Adding or Modifying an SNMPv3 User in CSS

When and where to use: Use this procedure to create, update, or delete an SNMPv3 user from the **Configure SNMPv3 Users** window.

Procedure:

1. From the **Configure SNMPv3 Users** window, to add or modify the selected SNMPv3 user, click one of the following:
   - **Create:** Creates a user when the status is Not Present.
   - **Update:** Updates an existing user.
   - **Delete:** Removes an existing user.

   NOTICE: The MotoZSS Username is used only in an ASTRO® 25 repeater site or Multisite subsystem.

   A **Confirmation** dialog box appears and prompts if you want to continue.
2. Click **Yes**.

   The **Processing Requests** dialog box appears and processes the request. A green square X indicates OK and a red square X indicates failure.
3. After reviewing the processing status, click **OK**.

   NOTICE: If you encounter any errors, go back to the appropriate step and correct the information entered.
4. Repeat these steps for any SNMPv3 users you wish to create, update, or delete.
5. Click **Cancel** to exit the **Configure SNMPv3 Users** window.

   The **Configure SNMPv3 Users** window closes, and the CSS main window returns.

4.5.5.3.2
Performing an SNMPv3 Connection Verification in CSS

When and where to use: When the SNMPv3 user credentials have been created, modified, or deleted, ensure that the device is properly configured for SNMPv3. Follow this procedure to verify the SNMPv3 connection.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.
2. When the passphrase prompt screen opens, select the configured security level and enter the required passphrases.
3. If the connection was successful, click **OK**.

4.5.5.4
Customizing the Login Banner in CSS

This procedure describes how to edit the login banner security notice.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.

2 From the menu, select **Security** → **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)**.

3 From the **Remote Access/Login Banner** screen, **Remote Access Configuration** tab, click the **Login Banner** tab.

4 Edit the text of the banner.

5 Click one of the following:

- **Refresh:** re-reads the original Login Banner text.
- **Apply:** saves the changes and keep the screen open.
- **OK:** saves the changes and close the screen.
- **Cancel:** closes the screen without saving the changes.

4.5.5.5

Setting the SWDL Transfer Mode in CSS

This procedure sets the Software Download Manager (SWDL) transfer mode.

When and where to use: Follow this procedure to set the SWDL transfer mode to Ftp (clear) or Sftp (secure) before performing a software download on the device.

NOTICE: The SWDL transfer mode must be set to **Ftp** (clear) if any PSC 9600, STR 3000, QUANTAR®, or ASTRO-TAC® 9600 device is present at a site.

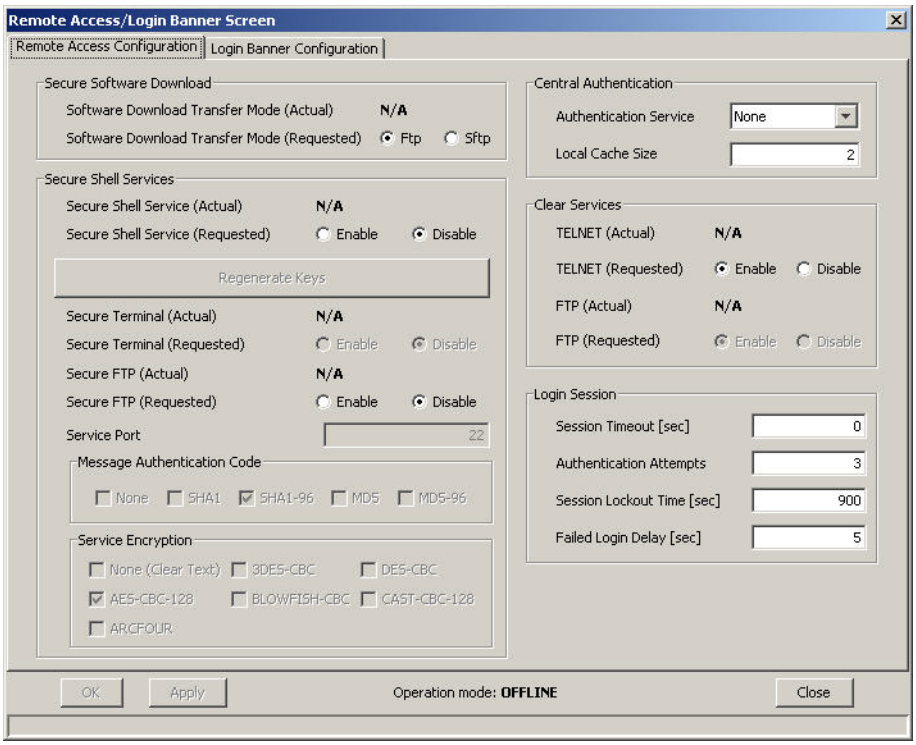
Procedure:

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.

2 From the menu, select **Security** → **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)**.

The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.

Figure 22: Remote Access Configuration Tab



3 In the **Software Download Transfer Mode (Requested)** field, choose either **Ftp** (clear) or **Sftp** (secure). Click **OK**.

NOTICE: Secure Shell Service (Requested) and Secure FTP (Requested) are automatically set to **Enabled** and grayed out when you choose **Sftp**.

4.5.5.6

Setting the Local Password Configuration in CSS

When and where to use: Use this procedure to set the complexity requirements and controls for the local service account password. The updated password criteria is enforced on the next password change for the device local service account. Password Configuration is an optional feature. For information, see “Password Configuration" in the *CSS Online Help*.

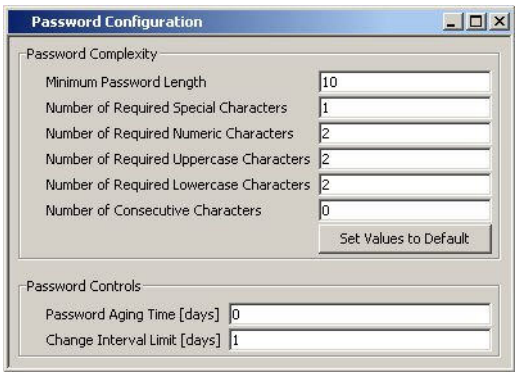
Procedure:

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 78.

2 In the navigation pane, click the **Password Configuration** element.

The **Password Configuration** window appears.

Figure 23: Password Configuration Window



3 Complete the following fields:

Minimum Password Length
This field allows you to enter a value as the minimum length for the password. The minimum can be between 8 and 255 characters, with a default of 10 characters.

Number of Required Special Characters
This field allows you to enter a value for the required number of special characters which must be included in the password. The value can be between 0 and 255, with a default of 1.

Number of Required Numeric Characters
This field allows you to enter a value for the required number of numeric characters which must be included in the password. The value can be between 0 and 255, with a default of 2.

Number of Required Uppercase Characters
This field allows you to enter a value for the required number of uppercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2.

Number of Required Lowercase Characters
This field allows you to enter a value for the required number of lowercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2.

Number of Consecutive Characters
This field allows you to enter the maximum number of consecutive repeated characters permitted in the password.

Set Values to Default
This field returns all fields to their system default values.

Password Aging Time [days]
This field allows you to enter a value between 0 and 65535 for the maximum number of days a local password is valid. After the **Password Aging Time** has elapsed, the password must be changed. The default value is 0.

Change Interval Limit [days]
This field allows you to enter a value between 0 and 65535 for the number of days which must elapse before a local password can be changed. The default value is 1.

4.5.6
CSS Configuration Parameters for a Trunked GCM 8000 Comparator

When and where to use:
Before proceeding with this process, complete the initial configuration of the device in Initial Configuration of a Device in CSS on page 73.

For configuration details for a trunked GCM 8000 Comparator site, see “Configuring GCM 8000 for Trunking Systems” in the Comparator Configuration & Service Help in the *CSS On-line Help*.

Process:

1. Connect to the comparator through an Ethernet port link and then read the configuration file from the comparator. See Connecting Through an Ethernet Port Link on page 78.
2. In the System tree, click **Zone** and complete the fields.
3. In the System tree, click **Site** and complete the fields.
4. In the System tree, click **Channel** and complete the fields.
5. In the System tree, click **Configuration** and complete the fields on the two tabs.
6. In the System tree, click **Network Services Configuration** and complete the fields on the three tabs.

   NOTICE: For configuration details for DNS and RADIUS Services, see the *Authentication Services* manual. For configuration details for SYSLOG Services, see the *Centralized Event Logging* manual.
7. In the System tree, click **Password Configuration** and complete the fields.

   NOTICE: Password Configuration is only required if you have passwords entered for local accounts. This sets the password complexity and controls. For details on password complexity and controls see “Password Configuration” in *CSS Online Help*.
8. From the menu, select **File** → **Save** to save the configuration data to a new archive file or select **File** → **Save As** to overwrite the existing archive file.

   IMPORTANT: Save any configuration changes to a local or network drive so that if the comparator module fails, the settings can be loaded to a replacement module. If the configuration file is not saved to a local or network drive, repeat the set-up steps after replacing a comparator module.
9. Write the configuration data to the comparator, as follows:
   - From the menu, select **File** → **Write Configuration to Device**.

4.5.7
CSS Configuration Parameters for a Conventional GCM 8000 Comparator

When and where to use:
Before proceeding with this process, complete the initial configuration of the device in Initial Configuration of a Device in CSS on page 73.

For configuration details for a conventional GCM 8000 Comparator, see “Configuring GCM 8000 for Conventional Systems” in the Comparator Configuration & Service Help in the *CSS On-line Help*.

Process:

1. Connect to the comparator through an Ethernet port link and then read the configuration file from the comparator. See Connecting Through an Ethernet Port Link on page 78.
2. In the System tree, click **Site** and complete the fields.
3. In the System tree, click **Channel** and complete the fields.
4. In the System tree, click **Configuration** and complete the fields on the three tabs.
5. In the System tree, click **Network Services Configuration** and complete the fields on the three tabs.

NOTICE: For configuration details for RADIUS Services, see the *Authentication Services* manual. For configuration details for SYSLOG Services, see the *Centralized Event Logging*, manual.

6 In the System tree, click **Password Configuration** and complete the fields.

NOTICE: Password Configuration is only required if you have passwords entered for local accounts. This sets the password complexity and controls. For details on password complexity and controls see “Password Configuration” in *CSS Online Help*.

7 From the menu, select **File** → **Save** to save the configuration data to a new archive file or select **File** → **Save As** to overwrite the existing archive file.

IMPORTANT: Save any configuration changes to a local or network drive so that if the comparator module fails the settings can be loaded to a replacement module. If the configuration file is not saved to a local or network drive, repeat the set-up steps after replacing a comparator module.

8 Write the configuration data to the comparator, as follows:

- From the menu, select **File** → **Write Configuration to Device**.

4.6 Configuring Centralized Authentication on Devices in VoyenceControl

When and where to use: This process provides the procedures for configuring centralized authentication on devices using the VoyenceControl component of the Unified Network Configurator (UNC) application.

NOTICE: VoyenceControl does not apply for a K core or non-networked site.

Process:

1 Configure Domain Name Service (DNS) on the device. See “DNS Configuration on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.

2 Configure Authentication Sources for the device. See “Centralized Authentication Configuration on RF Site and VPM Devices with VoyenceControl" in the *Authentication Services* manual.

3 Configure RADIUS parameters for the device. See “Configuring RADIUS on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.

4 Set the Local Cache Size for Centralized Authentication for the device. See “Setting the Local Cache Size for Central Authentication on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.

5 Enable/Disable Centralized Authentication for the device. See “Centralized Authentication Configuration on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.

6 Enable/Disable Centralized Event Logging for the device. See “Enabling/Disabling Centralized Event Logging on RF Site Devices and VPMs with EMC Smarts” in the *Centralized Event Logging* manual.

Chapter 5

GCM 8000 Comparator Optimization

This chapter contains optimization procedures and recommended settings relating to the GCM 8000 Comparator.

5.1 Setting the Link Delay Values

Procedure:

1. Connect the service computer/laptop to the comparator through the appropriate LAN switch either locally at a site or on the Network Management subsystem.
2. Connect to the comparator module using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 78.
3. From the menu, select **Service** → **Local Status Screen**.

   The **Local Status Screen** dialog box appears.
4. Click **Update Link Delay**.

   Link delay values are now measured by pinging each base radio and displaying the link delay values (in milliseconds). Afterwards the Link delay values are saved within the device.

   NOTICE: As a quick check of link integrity, this step can be repeated several times. Repeated Update Link Delay operations should return delay values within 2 msec tolerance for a given link.
5. From the menu, select **File** → **Write Configuration To Device**.

   A message stating `Write Device Successful` appears when the operation is complete.
6. Repeat this procedure for all other comparators in the system.

5.1.1 Ethernet Site Link Effects on Link Delay Values

When Ethernet site links are used between a Conventional Multi-Site prime site and the remote subsites, network jitter causes a variation in the link delay. As a result, a single link delay measurement using the CSS Set Link Delay Feature is not a reliable measure of the true link delay. The Set Link Delay procedure should be repeated several times to verify the accuracy of the link delay measurements. Otherwise, the link delay in the conventional comparator for each subsite can be manually entered into the conventional comparator Subsite Configuration tab using CSS.

Alternatively, for system configurations with ASTRO® 25 system Radio Network Management, the amount of link delay can be determined by examining the Ethernet Link Statistics in the UEM. See the *Unified Event Management* manual for information on viewing configured collections for a device. Specifically, the IPTD Maximum should be retrieved for each remote site gateway to determine the maximum round-trip IPTD measurements reported to the UEM over a specific time interval. Since the IPTD specifies round-trip delay, one-way link delay is approximately half of this value and should be determined by dividing the largest IPTD Maximum listed over the interval by 2. This value should be entered in the link delay CSS field for each subsite link. This procedure should be performed for each subsite.

This page intentionally left blank.

Chapter 6

GCM 8000 Comparator Operation

This chapter details tasks to perform once the GCM 8000 Comparator is installed and operational on your system.

6.1 Powering Up the GCM 8000 Comparator

Procedure:

1. Turn the power switch to the ON position.
2. Verify if the power LED is on.

6.1.1 GCM 8000 Comparator Power Supply and Battery Charger LEDs

Table 9: GCM 8000 Comparator Power Supply and Battery Charger LEDs

LED	Description	Indication	Status
On LED	Indicates that the power supply is delivering power to the chassis	Green	An appropriate amount of input voltage is supplied to the power supply and the switch is in the on position.
		Off	Appropriate power is not available for the power supply or the switch is in the off position.
Module Fail LED	Indicates a power supply failure.	Red	The power supply module has detected a malfunction, such as a shorted output, exceeded current limit, or loss of communication with the control module.

6.2 Powering Down the GCM 8000 Comparator

Procedure:

1. Set the power supply module switch to the OFF position.
2. If the comparator includes a battery backup, disconnect the battery revert cable from the rear of the chassis.

WARNING: Shock hazard. The GCM 8000 Comparator contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the comparator and remove the power cabling and any battery backup cabling when servicing this equipment.

6.3 GCM 8000 Comparator LED Indicators

The comparator module has several LEDs indicating the general conditions for the comparator and its traffic activities. For a quick status indication of the comparator equipment, visually inspect the LEDs.

Check the following for the overall comparator conditions:

- All LEDs momentarily light, following the comparator reset (Reset button on front panel) or upon comparator power up.
- If no LED indicators are **ON**, ensure that AC power to the comparator power supply is present. Check the circuit breaker at the AC source and the power cable.
- All LEDs flashing on and off indicate that the comparator is in **FLASH** mode.
- All LEDs flash up and down sequentially to indicate that the software is being loaded into **FLASH** memory.

6.3.1 GCM 8000 Comparator Service LEDs

Table 10: Trunked GCM 8000 Comparator Service GREEN LEDs

LED	Application Use	Green On	Green Blinking	OFF
1	Channel State	Voice	Control Channel or Packet Data	Idle or Disconnect
2	1PPS and sub-site links			1 PPS Operational and no subsite link failures
3	Rx Activity	Subsites	Subsites or Network	Not receiving
4	Tx Activity	Subsites	Subsites or Network	Not transmitting
5	SWDL / VLAN		Version validation or auto-VLAN detection	
6	Local (all FRUs)			Good - no faults
7	HW Active	Active		Inactive

Local = For the reporting purposes a FRU is considered to be a power supply, fan, or a subsite link.

Table 11: Trunked GCM 8000 Comparator Service AMBER LEDs

LED	Application Use	Amber On	Amber Blinking	OFF
1	Channel State	Failsoft NT	BSI or Failsoft	Idle or Disconnect
2	1PPS and sub-site links	See Note 1	See Note 1	1PPS Operational and no subsite link failures
3	Rx Activity			Not receiving
4	Tx Activity	Standby		Not transmitting

Table continued…

LED	Application Use	Amber On	Amber Blinking	OFF
5	SWDL/ VLAN	SWDL with common VLAN	SWDL with split VLAN	
6	Local (all FRUs)	Warning	Minor FRU failure	Good – no faults
7	HW Active			Inactive

Note 1: 1PPS or Subsite Link failure – for more details on the possible cause, use the Configuration/ Service Software (CSS) to view the technical log on the **Status Report Screen**.

Failsoft NT
= No Transmit, a failsoft state in which calls are disabled.

BSI
= Analog Base Station Identification state.

Local
= For the reporting purposes a FRU is considered to be a power supply, fan, or a subsite link.

Table 12: Trunked GCM 8000 Comparator Service RED LEDs

LED	Application Use	Red On	Red Blinking	OFF
1	Channel State	Disabled	V.52 test	Idle or Disconnect
2	1PPS and sub-site links	1PPS not present (comparator is not simulcast capable) and subsite link failures	See Note 1	1PPS Operational and no subsite link failures
3	Rx Activity			Not receiving
4	Tx Activity			Not transmitting
5	SWDL/ VLAN	Not in SWDL with split VLAN		
6	Local (all FRUs)	Critical FRU failure (hardware failure or a subsite is unreachable)	Major FRU failure	Good – no faults
7	HW Active			Inactive

Note 1: 1PPS or Subsite Link failure – for more details on the possible cause, use the Configuration/ Service Software (CSS) to view the technical log on the **Status Report Screen**.

Local
= For the reporting purposes a FRU is considered to be a power supply, fan, or a subsite link.

Table 13: Conventional GCM 8000 Comparator Service GREEN LEDs

LED	Application Use	Green On	Green Blinking	OFF
1	Links Status (network)	Network Link-Up and no V.52 test		Network Link Unconfigured and no V.52 test
2	1PPS and subsite links			1PPS Operational and no subsite link failures.
3	Rx Activity	Subsites	Subsites or Network	Not receiving
4	Tx Activity	Subsites	Subsites or Network	Not transmitting
5	SWDL			Not in SWDL
6	Local (all FRUs)			Good – no faults
7	HW Active	Active		Inactive

Local
= for the reporting purposes a FRU is considered to be a power supply, fan, or a subsite link.

Table 14: Conventional GCM 8000 Comparator Service AMBER LEDs

LED	Application Use	Amber On	Amber Blinking	OFF
1	Links Status (network)	Network Link-Up and V.52 test in progress	Network is failed or unconfigured and V.52 test in progress	Network Link Unconfigured and no V.52 test
2	1PPS and subsite links	See Note 1	See Note 1	1PPS Operational and no subsite link failures
3	Rx Activity			Not receiving
4	Tx Activity			Not transmitting
5	SWDL	SWDL		Not in SWDL
6	Local (all FRUs)	Warning	Minor FRU failure	Good – no faults
7	HW Active			Inactive

Note 1: 1PPS or Subsite Link failure – for more details on the possible cause, use the Configuration/ Service Software (CSS) to view the technical log on the **Status Report Screen**.

Local
= for the reporting purposes a FRU is considered to be a power supply, fan, or a subsite link.

Table 15: Conventional GCM 8000 Comparator Service RED LEDs

LED	Application Use	Red On	Red Blinking	OFF
1	Links Status (network)	Network Link-Down and no V.52 test		Network Link Unconfig-ured and no V.52 test
2	1PPS and sub-site links	1PPS not present (com-parator is not simulcast ca-pable) and subsite link failures	See Note 1	1PPS Operational and no subsite link failures
3	Rx Activity			Not receiving
4	Tx Activity			Not transmitting
5	SWDL			Not in SWDL
6	Local (all FRUs)	Critical FRU failure (hard-ware failure or a subsite is unreachable)	Major FRU failure	Good – no faults
7	HW Active			Inactive

Note 1: 1PPS or Subsite Link failure – for more details on the possible cause, use the Configuration/ Service Software (CSS) to view the technical log on the **Status Report Screen**.

Local
= for the reporting purposes a FRU is considered to be a power supply, fan, or a subsite link.

Whenever the Comparator cannot detect 1PPS signal on its “1PPS input” connector, 1PPS fault is reported. Subsite link failure is reported, if there is a subsite link enabled and there is no response from the corresponding subsite.

NOTICE: The 1PPS input on the rear of the GCM 8000 Comparator is high impedance. An external termination is needed to properly terminate the cable connected to the input. It is recommended that a BNC "T" and a 50 Ohm BNC termination connect to the input to terminate the cable.

6.3.2
GCM 8000 Comparator Status and Alarm LEDs

The status and alarm LED assignment for the GCM 8000 Comparator are shown and definitions for each status follow the assignment table.

Table 16: GCM 8000 Comparator Status and Alarm LED Assignment

LED	No Pow-er	Lamp Test	Failure	Impaired	Booting Up	Online
Status LED (green)	Off	On	Off	On	Flash	On
Alarm LED (red)	Off	On	On	Flash	Off	Off

Table 17: GCM 8000 Comparator Status/Alarm LEDs Definitions

Status	Definitions
No Power	The device is currently without power, both primary power and auxiliary power. The No Power state tells the service technician that there is a fundamental problem.
Lamp Test	The Lamp Test state is used to verify if the indicators are operational.
Booting Up	The Booting Up state indicates that the device is booting or is undergoing diagnostics and is not yet ready to place into service. Even though no failure or impairment is identified, the device is not ready to place into service.
Online	The comparator is fully operational. The Online state is used to indicate that the comparator is fully operational. It may be in an Enabled or User-Disabled mode. The Online state indicates that the comparator should not be removed as it is possibly involved in active calls.
Impaired	The comparator is not fully operational due to internal or external causes. Some corrective action must be taken to return to 100% functionality.
Failure	This status indicates a failure fixed only through a replacement. The exception to this rule is lack of the 1PPS reference signal on “1PPS input” connector. If something other than a hardware fault or missing 1PPS signal is causing the state, the status is Impaired.

6.3.3
GCM 8000 Comparator Switch or Active/Inactive Status LEDs

The four active/inactive status LEDs are found on the top of the service port area of each comparator module. They are visible by opening the service door.

Table 18: GCM 8000 Comparator Active/Inactive Status LEDs

Active/Inactive LEDs	Description
SW	Indicates internal activity.
CPU	Indicates CPU activity.
CP2	Not in use
RCPU	Not in use

Table 19: GCM 8000 Comparator Active/Inactive LEDs

Information State	Link Status LED
Link Inactive	Off
Link Established (assumes no activity)	Green
Link Active	Yellow or Amber

6.3.4
GCM 8000 Comparator Link LEDs

Table 20: GCM 8000 Comparator Link LEDs

LED	Link Inactive	Link Established (assumes no activity)	Link Active
Activity LED (amber)	Off	Off	Amber – constant
Link LED (green)	Off	Green – constant	Green – constant

6.3.5
GCM 8000 Comparator Power Supply LEDs

The power switch on the front of the power supply is used to enable or disable the DC outputs of the power supply for the GCM 8000 Comparator.

The power supply has three LEDs, which provide a visual image of the operating condition of the power supply.

Table 21: GCM 8000 Comparator Power Supply LEDs

LED	Explanation
Alarm	Red LED: When illuminated, it indicates the power supply is no longer operating within its design specifications.
Status	Green LED: When illuminated, it indicates the power supply is operating within its design specifications.
Fan	Red LED: When illuminated, it indicates the fan for the power supply is no longer functioning as per its design specifications.

6.3.6
GCM 8000 Comparator Fan Assembly LEDs

The fan assembly has one LED, the Fan Alarm, on the front in the corner. The LED provides a visual image of the operating condition of the fan assembly.

Table 22: GCM 8000 Comparator Fan Assembly LEDs

LED color	Explanation of State
Off	Operational, or Off
Red (constant)	Failure

6.4
CSS Status Window

This section explains CSS Status Window for the GCM 8000 Comparator.

The CSS Status Window identifies the status of the comparator objects:

- Comparator
- Power Supply

- Fan
- Infrastructure Link

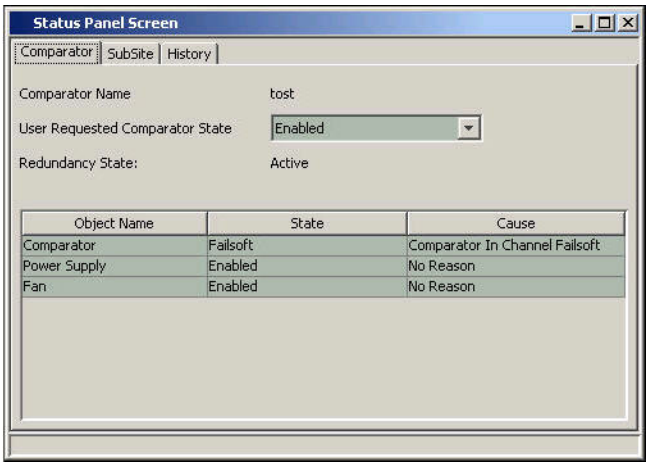
6.4.1
Enabling the CSS Status Window

Procedure:

1. Connect to the comparator through an Ethernet connection. See Connecting Through an Ethernet Port Link on page 78.
2. From the menu, select **Service** → **Status Panel Screen**.

   The **Status Panel Screen** window appears.

   Figure 24: GCM 8000 Comparator – Status Panel Screen



6.4.2
Functions of the CSS Status Window

The comparator name appears on the **Status Panel Screen**. This name is specified through Configuration element in the Navigation Pane.

The Comparator State is changed in the **User Requested Comparator State** list box. There are three possible states:

- **Enabled:** The comparator is able to process calls.
- **User Disabled:** For a non-redundant comparator, the comparator is not allowed to process calls. If in a redundant configuration, after disabling, the comparator isolates itself from the other comparator and the RNG. If the comparator was the active comparator and the standby comparator is not isolated from the system, then the standby comparator becomes active and takes over operations at the site.

  NOTICE: The User Disabled state is not available for a conventional comparator.

- **Restart:** The comparator resets.

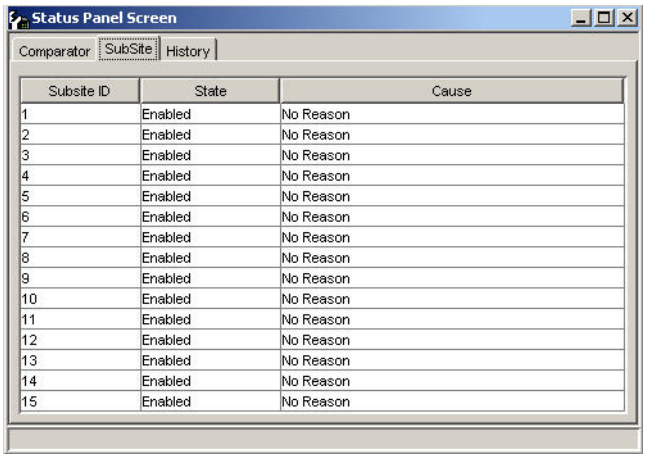
The redundancy state of a trunked comparator is shown as either **Active** or **Standby**.

The states and causes of comparator FRUs are also presented here. The actual state and possible cause of the comparator, power supply, and fan failure can be observed.

The **SubSite** tab is used to observe the actual state and possible cause of SubSite link objects.

NOTICE: Subsite states and causes are not shown for standby comparators.

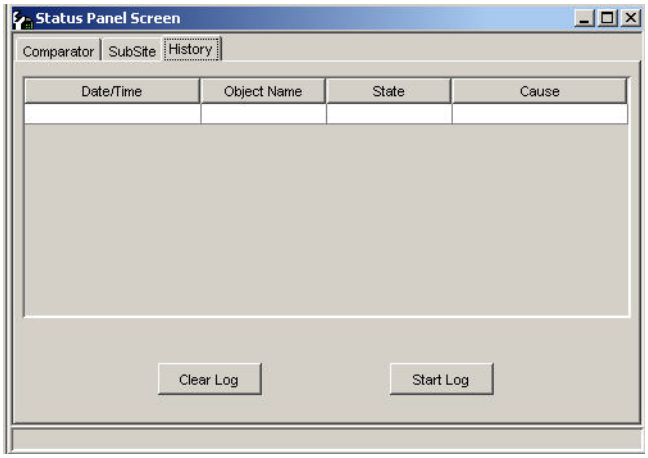
Figure 25: GCM 8000 Comparator – Status Panel Subsite Screen



The **History** tab is used for when State-Change events coming from the comparator can be observed. Each event is presented by the following values:

- Date/Time
- Object Name
- State
- Cause

Figure 26: GCM 8000 Comparator – Status Panel History Screen



GCM 8000 Comparator objects are Comparator, Power Supply, Fan, and SubSite links. The trap log history can be cleared by clicking **Clear Log**. Incoming traps can be saved to a log file by clicking **Start Log**.

This page intentionally left blank.

Chapter 7

GCM 8000 Comparator Maintenance

This chapter describes periodic maintenance procedures relating to the GCM 8000 Comparator.

7.1 Fan Grill Cleaning Instructions

If the station equipment is installed in a dusty environment, take precautions to filter the air used for a forced cooling of the station. Excessive dust drawn across and into the device circuit modules by the cooling fans can adversely affect heat dissipation and circuit operation. In such installation, be sure to clean or replace external filtering devices periodically.

If dust has accumulated on the fan grills, cleaning the fan grills is recommended. When cleaning, take care to prevent dust from being pulled into the modules. Use a damp cloth to wipe the front of the fan grills. When removing the power supply, turn off the unit before proceeding.

This page intentionally left blank.

Chapter 8

GCM 8000 Comparator Troubleshooting

This chapter provides fault management and troubleshooting information relating to the GCM 8000 Comparator.

8.1 Troubleshooting the GCM 8000 Comparator

Table 23: GCM 8000 Comparator – General Troubleshooting

Problem	Troubleshooting
General connectivity problems	**1** If you have access to the equipment, check the LEDs to verify if each piece of equipment is connected and operational. **2** In the CSS, check the alarms of the comparator and all associated devices and links. **3** Verify the configuration of the comparator through UNC and CSS. Verify if the IP address, the subnet mask, and the default gateway for the comparator is correct. In the CSS, send a diagnostic command to enable the comparator. **4** For a conventional comparator, verify that the DNS Hostname for the comparator is correct. If the DNS Hostname was incorrect and then corrected, further corrections may be needed on the DNS server, UNC, and UEM. See the "Troubleshooting" chapter in the *Authentication Services* manual. **5** Verify if the physical cabling is firmly connected and is in good condition. Check for any sharp bends or kinks in cabling. Test suspected cabling for noise, continuity, attenuation, and crosstalk. Replace the cabling if necessary. **6** If the connection fails to operate normally, check the diagnostics, and if needed, contact the Motorola Solutions Support Center (SSC). **7** If the comparator still fails to operate properly, create a backup of the current configuration, then reinstall the software and reconfigure the comparator. **8** Replace the comparator if necessary.

Table continued…

Problem	Troubleshooting
Unit does not power up	**1** If you have access to the equipment, check the LEDs to verify if each piece of equipment is connected and is operational. **2** Check the power cabling and verify if the power source for the comparator is supplying the appropriate voltage. Connect the comparator to another power source or replace the power cabling if necessary. Check all power sources if there is more than one. **3** Check for any burn marks or physical damage to the comparator and check whether the comparator is properly grounded.
Unable to perform a password reset	If the device module has been replaced and serial port access is not available to configure the IP address, the device may have the account locked out or the backplane slot has passwords enabled. Perform the following steps: **1** Move the board module to a different chassis or to a different slot in the backplane where local passwords are not configured. **2** Configure the IP address and reset the device through the front panel RS-232 serial service port using CSS. **3** Perform the local password reset operation (to clear account information stored in the FRU) through and Ethernet port link using CSS. **4** Move the board module back to the original chassis or slot. **5** Perform the local password reset operation again (to clear account information stored in the backplane).

8.2 Software Troubleshooting Tools

Several tools are available for troubleshooting the GCM 8000 Comparator:

- Unified Event Manager to Monitor Links and Components
- Unified Network Configurator for Troubleshooting
- MOSCAD NFM
- Configuration/Service Software (CSS)

NOTICE: The Unified Event Manager (UEM) can be established as a more centralized fault management solution replacing the MOSCAD GMC. See the *Unified Event Manger* manual and the *UEM GMC MOSCAD Transition Guide* for details.

8.2.1

Troubleshooting GCM 8000 Comparator Alarms in Unified Event Manager

Unified Event Manager (UEM) is a fault management software tool that displays alarms for devices in the subsystem. For further details on the UEM, see the *UEM Online Help*.

The comparator monitors the state and activities throughout the site, and reports any relevant events to UEM. The comparator also reports the status and events of its subcomponents including the power supply and fan.

Table 24: GCM 8000 Comparator Diagnostic Options

Option	Description
User Disable	Requests that the selected comparator disable (trunked only). If in a redundant configuration, after disabling, the comparator isolates itself from the other comparators and the RNG. If the comparator was the active comparator and the standby comparator is not isolated from the system, then the standby comparator becomes active and takes over operations at the site.
Enable	Requests that the selected comparator enable.
Restart	Requests that the comparator perform a reset. The comparator resets back in its current state.

8.2.1.1

Monitoring Links and Individual Components in Unified Event Manager

Use the Unified Event Manager (UEM) to monitor critical links and components in a device or in the system. Monitoring may take place remotely from a central operations center. Two types of monitoring include:

- Real-time monitoring of UEM Topology maps, which alert the user the “highest severity” of alarms of a particular subnet as they occur.
- Evaluation of UEM Active Alarms Window on a regularly scheduled basis.

See the *Unified Event Manager* manual or *UEM Online Help* for further details.

8.2.1.2

Analyzing Unified Event Manager Active Alarms Window

The Unified Event Manager (UEM) **Active Alarms** Window is useful for troubleshooting, because it captures alarms that may occur intermittently or during off-hours. For example, review the **Active Alarms** Window to correlate the reported loss of service with patterns of critical alarms, for the links and equipment.

When analyzing the **Active Alarms** Window, look for these types of patterns:

- Failures sent with time stamps on or about the same time.
- Failures from equipment attached to particular links. For example, routers, switches, base radios, site controllers, and comparators.
- Many devices are capable of sending out events that report both critical and non-critical events. Learn to distinguish between critical and non-critical events.

See the *Unified Event Manager* manual or *UEM Online Help*.

8.2.2
Device Troubleshooting in Unified Network Configurator

Use the Unified Network Configurator (UNC) to verify configuration data during system commissioning and later when you maintain or expand the system. Use UNC to do the following to the device:

- Verify configuration
- Correct configuration errors

See the *Unified Network Configurator* manual for further details.

8.2.3
MOSCAD Network Fault Management

If MOSCAD Network Fault Management (NFM) equipment is supported at the site, additional status, and alarm information for a device can be viewed through the MOSCAD NFM.

Figure 27: MOSCAD Network Fault Management – Example

When an alarm condition occurs, the alarm device for one of the modules begins to flash red. Selecting the LED box opens an alarm pop-up window indicating details of the alarm. To view the status of all alarms for a particular module within the device, select the alarm LED box corresponding to the particular module. Alarms can be acknowledged by pressing the **Acknowledge** button on the screen.

See the *MOSCAD Network Fault Management Feature Guide* for details.

NOTICE: The Unified Event Manager (UEM) can be established as a more centralized fault management solution replacing the MOSCAD GMC. See the *Unified Event Manger* manual and the *UEM/GMC Transition Setup Guide* for details.

8.2.4
Configuration/Service Software (CSS)

The GCM 8000 Comparator can be locally or remotely configured or serviced through Configuration/Service Software (CSS). CSS provides access to alarms, status information, configuration settings, and diagnostics for the GCM 8000 Comparator.

Use CSS for the following tasks which may be useful when troubleshooting the comparator. See the *CSS Online Help* for the GCM 8000 Comparator for specific details and instructions when using these tasks:

- Enable and disable channels and services (trunked comparator only)
- Saving or installing the comparator configuration data
- View and save a log of comparator alarms
- Determine comparator hardware and software versions
- Verify fan and power supply operation
- Determine Dynamic Frequency Blocking (DFB) status (trunked comparator only)
- Equalize the batteries
- Gather troubleshooting information that can be escalated to Motorola Solutions for evaluation
- Verify that the VLAN connections match with the comparator (trunked comparator only)

IMPORTANT: Before attempting to cycle power the comparator, save all relevant reports. Alarm data resides in the memory of the comparator and not saving it before cycling power results in loss of valuable troubleshooting data.

8.2.5
Local Password and SNMPv3 Passphrase Troubleshooting

The password reset mechanism in the Configuration/Service Software (CSS) application can be enabled/disabled. See “Secure Remote Access Configuration > Device Security Configuration - Security Services (Serial)” in the *CSS Online Help* for information. To obtain the keys for resetting either password or SNMPv3 passphrases for the device, contact Motorola Solutions Support Center (SSC).

NOTICE: The default values for the local passwords and SNMPv3 passphrases, as well as the keys for the local password reset procedure, may vary by system release. These default values and keys are treated as sensitive information and are provided to your organization through secured communication.

Table 25: Local Password and SNMPv3 Passphrase Troubleshooting

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Log-in Password
User is locked out of the local login, but knows SNMPv3 passphrases	✔	✘	See the *CSS Online Help* “SNMPv3 User Configuration”.	See the *CSS Online Help* “Resetting Device Passwords.”
User knows the local login, but not	✘	✔	See the *CSS Online Help* “Reset SNMPv3	See the *CSS Online Help* “Device Security

Table continued…

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Log-in Password
the SNMPv3 passphrases			Configuration (Serial)".	Configuration – Security Services (Serial)".
User knows both passphrases and local service password	✔	✔	See the *CSS Online Help* "SNMPv3 User Configuration".	See the *CSS Online Help* "Device Security Configuration – Security Services (Serial)".
User does not know SNMPv3 passphrase nor service account password	✘	✘	Contact Motorola Solutions SSC.	Contact Motorola Solutions SSC.

8.3
Hardware Troubleshooting Tools

This section explains the hardware troubleshooting tools (LED indicators) for the GCM 8000 Comparator.

8.3.1
LED Indicators - Troubleshooting Mode

See GCM 8000 Comparator LED Indicators on page 94 in the Operation chapter.

8.4
Failure of a Trunked GCM 8000 Comparator

The following are the general sequence of activities when the GCM 8000 Comparator fails:

1 The channel that was assigned to the comparator, becomes unavailable.

2 Behavior for other devices in the system is similar to the behavior during a CM-SC and CM-MSBR link failure.

3 MSUs that operate on the site, search for the available control channel. If there is no available control channel, then the MSUs become out of range.

4 If the comparator recovers, the channel becomes available again.

8.5
Failure of the Active Trunked GCM 8000 Comparator

If the active comparator fails, and the standby comparator has a connection with the master site, then a comparator switchover occurs. During the switch over period, the standby comparator re-initializes and becomes the active comparator.

During the comparator switchover process, the system exhibits dropped calls or Illegal Carrier state. The general sequence of activities during active comparator or LAN switch failure is explained in the following:

1 The channel that was assigned to the comparator becomes unavailable.

2 The standby comparator detects the loss of the active comparator within 2 seconds.

3 The new active comparator performs an initialization process (similar to the power-up initialization). During the switchover, calls in progress on those channels are interrupted or terminated. If a radio remains keyed on a failed channel during the switch over, the base radio might enter Illegal Carrier state as it would for existing Illegal Carrier scenarios.

4 After the switchover occurs, the channel becomes available and radio users and console operators will be able to place and receive calls on these voice/data channels.

8.6 Failure of Active and Standby Trunked Comparators

The following are the general sequence of activities when both active and standby comparators fail:

1 The channel that was assigned to the comparator becomes unavailable.

2 Behavior for other devices in the system is similar to the behavior during a CM-SC and CM-MSBR link failure. All the channels at the site dekey and the broadcast information ceases or enters Local Failsoft mode, depending on how the base radio is configured.

3 MSUs that operate on the site, search for the available control channel. If there is no available control channel, then the MSUs become out of range.

4 If one or both comparators recover, the first comparator to recover initializes and becomes the active comparator. Once both comparators have recovered, however, the active/standby states are automatically updated in accordance with the “redundancy preferred” activation logic described earlier.

For additional information on Local Failsoft, see the *Trunked IP Simulcast Subsystem Remote Site* manual.

8.7 Failure of a Conventional GCM 8000 Comparator

The following are the general sequence of activities when a conventional GCM 8000 Comparator fails:

1 The channel that was assigned to the comparator becomes unavailable.

2 If the comparator recovers, the channel becomes available again.

3 Fallback in-cabinet repeat mode (base radio), if configured, operates during a comparator or prime-to-remote site link failure.

8.8 Reset Button

Each GCM 8000 Comparator module has a **RESET** button on the front, accessible through the drop-down door to the left of the fan.

The **RESET** button is used to reboot the device. Pressing the button for more than 3 seconds results in a reset or reboot of the comparator module. The button is set into the chassis, so it is difficult to accidentally engage.

8.9 Motorola Solutions Support Center

Motorola Solutions Support Center (SSC) can help technicians and engineers resolve system problems, and ensure that warranty requirements are met. Check your contract for specific warranty information.

Motorola Solutions assigns a tracking ticket number that identifies each support call. This ticket number allows Motorola Solutions to track problems, resolutions, and activities for the call, and if possible, communicate the resolution and a status of call so that the SSC can note the resolution and close the ticket.

8.9.1
Information Necessary to Contact Motorola Solutions Support Center

Before calling the Motorola Solutions Support Center (SSC), log all steps taken to troubleshoot the problem and any results of those steps. The SSC can use this information to determine the appropriate support actions.

Listed is the following information to collect before calling the SSC:

- System ID number (such as 2CB5). Each zone in the system has a unique system ID number
- Location of the system
- Date the system was put into service
- Software and firmware versions
- Symptom or observation of the problem, such as:
  - When did it first appear?
  - Can it be reproduced?
  - Are there any other circumstances contributing to the problem (for example, loss of power)?
- Maintenance action preceding the problem, such as:
  - Upgrade of software or equipment
  - Changes to hardware or software configuration
  - Reload of software from a backup disk, CD, or DVD with the version and date

Dispatch Support:

- Site ID
- Description of problem
- Severity of issue

Tech Support:

- Site ID
- Billing information (If not being billed under contract)
- Name or model number of product causing the issue (Helps get you over to proper tech support group)

Return Authorization:

- Site ID
- Part Number and/or description of part
- How being billed
- Where it is being billed
- Where it is being shipped

8.9.2
Where to Call for Service

After collecting the required information and writing a detailed problem report, contact the Motorola Solutions Support Center (SSC) to help with the problem.

8.9.2.1
Motorola Solutions Support Center

The Motorola Solutions Support Center (SSC) is the primary Motorola Solutions contact. Call Motorola Solutions SSC:

- Before any software reload
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) or Field Replaceable Equipment (FRE) to repair the system

Motorola Solutions SSC contact information:

- Phone: (800) 221-7144 for domestic calls and (302) 444–9800 for international calls
- Fax: (847) 725-4073

8.9.3
Subcontractors

The Motorola Solutions Service Subcontractor Assessment program ensures that service people Motorola Solutions contracts meet strict minimum requirements before they can work on any system. For more information on this program, contact the Motorola Solutions representative.

This page intentionally left blank.

Chapter 9

GCM 8000 Comparator FRU/FRE Procedures

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs), and includes replacement procedures applicable to the GCM 8000 Comparator.

9.1 Required Tools and Equipment

The following items are necessary to bring to the replacement site when replacing any equipment:

- Electrostatic discharge (ESD) strap (Motorola Solutions part number RSX4015A, or equivalent)
- Service computer/laptop with Configuration/Service Software and Software Download Manager applications installed
- DB-9 Straight through serial cable
- Ethernet patch cable
- Crosstip and slotted screwdrivers
- TORX® driver set
- 1/2 drive torque wrench capable of torque settings to 110 in/lbs.

9.2 Field Replaceable Units (FRUs)

This section covers FRU kit numbers, part numbers, and procedures for replacing the FRUs.

Table 26: GCM 8000 Comparator Field Replaceable Units

Component Type	FRU Kit Number
GCM 8000 Comparator module	DLN6966A
GCM 8000 Comparator Fan Assembly	DLN6898A
GCM 8000 Comparator Power Supply for DLN6966A	DLN6781A (0182516W14) or DLN6805A (0182516W20)
GCM 8000 Comparator Power Supply for DLN6569A	DLN6781A (0182516W14)

Table 27: GCM 8000 Comparator Part Numbers

Component Type	Part Number	From where to order
GCM 8000 Comparator Backplane	0180706H87	Order from North America Parts Organization only
GCM 8000 Comparator Power Supply Fan	5985167Y02	Order from North America Parts Organization only

9.3 Replacing the GCM 8000 Comparator Module

IMPORTANT: The comparator module can be hot swapped, but causes loss of functionality.

Prerequisites:
Before replacing the comparator module, pull configuration and hardware information from the comparator into the Unified Network Configurator (UNC) by performing a “Pull All” procedure. See the “Scheduling the Pull of Device Configurations” section in the *Unified Network Configurator* manual. This step may not be possible if communication is severed between the comparator and the UNC or if the comparator is in a K core or non-networked site.

Procedure:

1. Wear an Electrostatic Discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear this ESD strap throughout this procedure to prevent ESD damage to any components.

2. Locate the comparator module being replaced.
3. If the comparator module is non-operational, go to step 7.
4. Connect to the comparator module using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 78.

   NOTICE: If all unused ports on the LAN switch are disabled, enable the desired port. See the *System LAN Switches* manual.

5. Save the comparator configuration to the service computer/laptop as follows:
   a. From the menu, select **File** → **Read Configuration From Device**.
   b. At the success message, click **OK**.
   c. From the menu, select **File** → **Save As**.
   d. On the **Properties Screen**, enter the IP address of the comparator. Click **OK**.
   e. On the **Save** window, select the directory where you want to save the configuration file, type a meaningful name for the file (use `.cpl` as the extension or do not type an extension). Press ENTER.

   The comparator configuration is saved to the location you indicated. The configuration file is reloaded later to the replacement comparator module.

6. For a trunked comparator module, disable the channel before replacing the module so the system does not attribute the loss of channel to a failure. Disable the comparator as follows:

   NOTICE:
   It is not necessary to turn off the power supply for the comparator module being replaced, as the modules can be swapped out with the power on.

a From the menu, select **Service** → **Status Panel Screen**.

The **Status Panel Screens** window appears.

b Select the **Comparator** tab.

c From the **User Requested Comparator State** list box, select **User Disabled**.

The comparator is disabled.

7 Disconnect the LAN switch Ethernet cable from the Net AUX on the comparator module being replaced.

8 Remove the fan assembly to gain access to the comparator module. See Replacing the Fan Assembly on page 120.

IMPORTANT: The comparator module can be swapped out without shutting the power off. The fan assembly, however, must be in place within a reasonable amount of time so the comparator module does not overheat and shut down.

9 Using a T20 bit, loosen the two captive screws on the front of the comparator module to disengage them from the chassis.

10 Using the handle, gently pull the module straight out along the guides on which it sits.

11 Slide in the replacement comparator module along the guiding rails until it is engaged. A slight push is needed to engage the module.

IMPORTANT: If the comparator module stops well before it is engaged, it is in an incorrect position. Either it is in the wrong slot or it is rotated 180 °. The module has a keying feature that prevents it from going all the way into an incorrect slot, or going into the correct slot but rotated 180 °. Do not try to force the module.

12 Using a T20 bit, tighten the two captive screws on the front of the module to secure the comparator module to the chassis.

13 Reconnect the LAN switch Ethernet cable to the Net AUX on the replacement comparator module.

14 Reinstall the fan assembly unit. See Replacing the Fan Assembly on page 120.

15 Perform basic device configuration in CSS using the serial port. See Connecting Through a Serial Port Link on page 74.

a Set the **IP Address** and **BR_CM Pairing Number** for the device. See Setting the Device IP Address and Pairing Number in CSS on page 75.

b Set the serial security services. See Setting the Serial Security Services in CSS on page 77.

16 On systems with MAC Port Lockdown implemented, disable MAC Port Lockdown. The switch port where the colocated replacement device is connected to needs to be Unlocked before connecting with CSS or performing a software download. See the *MAC Port Lockdown* manual for instructions on how to disable MAC Port Lockdown.

17 Open the Software Download Manager application, and perform the following:

CAUTION: Make sure to load the correct version of the software. There is a possibility of a mismatch in software versions when replacing the comparator module with an on-hand spare. If a mismatch in software versions occurs, this may cause the comparator to go into a configuration mode of operation with a reason of 'Invalid Software Version'. If this occurs, the comparator must be reset.

a From the **Advanced Options** menu, select the transfer type.

b From the menu, select **File** → **File Manager**.

The **Software Depot File Manager** opens.

c From the menu, select **Component Operations** → **Import Fileset**.

The **Import a Fileset Into the Software Depot** dialog box appears.

d Click **Browse** and search for the `swdlv3.cfg` file, or follow path: `E:\swdl\swdlv1.cfg` or `swdlv3.cfg`. Click **Open**.

The file appears in the **Configuration File Path** field of the dialog box.

e Click **Generate**. Click **OK**.

The **Import a Fileset Into the Software Depot** dialog box closes and the software component appears in the **Components In the Software Depot** list of the **Software Depot File Manager** window.

f Exit the **Software Depot File Manager**.

18 For a conventional device, perform a single device software download to transfer and install the latest comparator software using Software Download Manager, as follows:

a Click **Open Single Device Mode**.

b Enter the ***<IP address>*** of the device. Click **Connect**.

A **Security Level** screen appears.

c Choose the required security level. Click **OK**.

d In the **Select an Option** drop down list, select **Upgrade**.

e In the **Operation Type** drop down list, select **Transfer and Install**.

f In the **Application Type**, select the application to install.

g In the **Software Version** drop down list, select the appropriate software version.

h In the **Bank Selection** drop down list, select the bank to receive the software. Select **Automatic** to store the software in the bank that is more suitable for the device.

i Click **Start Operation**.

j In the window that appears, click **Proceed**.

If the transfer was successful, the progress bar in the **Operation Status** tab displays green. If the transfer failed, the progress bar displays red

19 Perform a site software download for trunked comparators. See Performing a Site Download on page 127.

A site software download is not available for conventional devices.

CAUTION: It is crucial that a site software download is performed at the site to ensure that all devices are on the same software version, VLAN, and active bank. Failure to perform this step results in the replacement comparator channel to have a mismatch in software versions. If a mismatch in software versions occurs, the comparator may go into a configuration mode of operation with a reason of ‘Invalid Software Version’. If this occurs, the comparator must be reset.

20 Disconnect the service computer/laptop from the serial port of the comparator.

21 Perform basic device configuration in CSS using an Ethernet connection. See Connecting Through an Ethernet Port Link on page 78.

a Set the BR/CM Pairing Numbers. See Setting the BR/CM Pairing Number in CSS on page 81.

b Set the current date and time. See Setting the Date and Time in CSS on page 82.

c Set the local password configuration (optional). See Setting the Local Password Configuration in CSS on page 87.

22 Complete the configuration of the Information Assurance features, as follows:

a Change the SNMPv3 configuration and user credentials. See Changing SNMPv3 Configuration and User Credentials in CSS on page 82.

b Create, update, or delete an SNMPv3 user. See Adding or Modifying an SNMPv3 User in CSS on page 85.

c Verify the SNMPv3 credentials. See Performing an SNMPv3 Connection Verification in CSS on page 85

d Set the SWDL transfer mode. See Setting the SWDL Transfer Mode in CSS on page 86.

e Configure Domain Name Services (DNS). See Chapter 7, “Configuring DNS with CSS” in the *Authentication Services* manual.

f Configure for Secure SHell (SSH). See Chapter 4, “Configuring SSH Devices at an RF Site” in the *Securing Protocols with SSH* manual or see “Device Security Configuration – Remote Access/Login Banner (Ethernet)” in the *CSS Online Help*.

g Restore the following Clear Protocols parameters in the Remote Access Configuration tab on the Device Security Configuration screen in CSS. See “Device Security Configuration – Remote Access/Login Banner (Ethernet)” in the *CSS Online Help*.

h Enable RADIUS Authentication. See Chapter 7, “Configuring RADIUS Sources and Parameters with CSS” in the *Authentication Services* manual.

i Enable Centralized Authentication. See Chapter 7, “Enabling/Disabling Centralized Authentication with CSS” in the *Authentication Services* manual.

j Set the Local Cache Size for Centralized Authentication. See Chapter 7, “Setting the Local Cache Size for Central Authentication with CSS” in the *Authentication Services* manual.

k Enable Centralized Event Logging (if required by your organization). See Chapter 6, “Enabling/Disabling Centralized Event Logging on Devices with CSS” and Chapter 1, “Event Logging Client Configuration” for proper hostnames in the *Centralized Event Logging* manual.

23 From CSS, restore the Codeplug Archive from backup. Reload the configuration into the new device, as follows:

a From the menu, select **File** → **Open**.

b Locate and select the previously saved configuration file for the comparator module.

NOTICE: If you were not able to back up the configuration from the previous comparator module, you can use the configuration from your system build book or use the default configuration file for the comparator module. Specific settings for the comparator module must still be configured. See the *CSS Online Help* for detailed configuration instructions.

c On the **Properties** window, click **OK**.

d When the **Progress Monitor** screen is complete, click **OK**.

e From the menu, select **File** → **Write Configuration To Device**. Click **OK**.

f On the Ethernet connection confirmation screen, click **OK**.

g On the **Connection** screen, enter the ***<IP Address>*** and click **Connect**.

h On the **SNMPv3 PassPhrase Prompt** dialog box, enter the **User Information** and **Passphrase Information**. Click **OK**. If Authentication Services are not enabled on a device, click **OK** when the dialog box appears.

i On the confirmation screen, click **OK**.

j When the **Progress Monitor** screen is complete, click **OK**.

The configuration from the file you selected is loaded into the new comparator module.

24 Read the comparator, as follows:

a From the menu, select **File** → **Read Configuration From Device**.

b One the confirmation screen, click **OK**.

c When the **Progress Monitor** screen is complete, click **OK**.

25 For a trunked comparator module, enable the comparator module as follows:

a From the menu, select **Service** → **Status Panel Screen**.

The **Status Panel Screen** window appears.

b Select the **Comparator** tab.

c From the **User Requested Comparator State** list box, select **Enabled**.

The comparator module is enabled after approximately two minutes.

26 On systems with MAC Port locking, disable the locking and then re-enable the locking with the MAC address of the comparator. The device being replaced may be connected to an Ethernet port on a switch which implements MAC Port locking (HP switch or site controller). If so, the Ethernet switch port must be unlocked and relocked to the MAC address of the replacement device. See the *MAC Port Lockdown* manual for instructions on how to disable and enable MAC port locking.

NOTICE: Following the device restoration, if it was connected to an HP switch port, the HP switch port may have been disabled due to an unexpected MAC address. If so, re-enable the port on the HP switch.

27 Replace the comparator in Unified Network Configurator (UNC). See Chapter 4, “Replacing a Device” in the *Unified Network Configurator* manual.

28 Discover the comparator in the UEM. See the *Unified Event Manager* manual.

29 Verify that the comparator module is operating properly:

- The Status LED on the front of the new comparator module is green.
- Proper operation is confirmed using software tools, such as UEM and CSS.

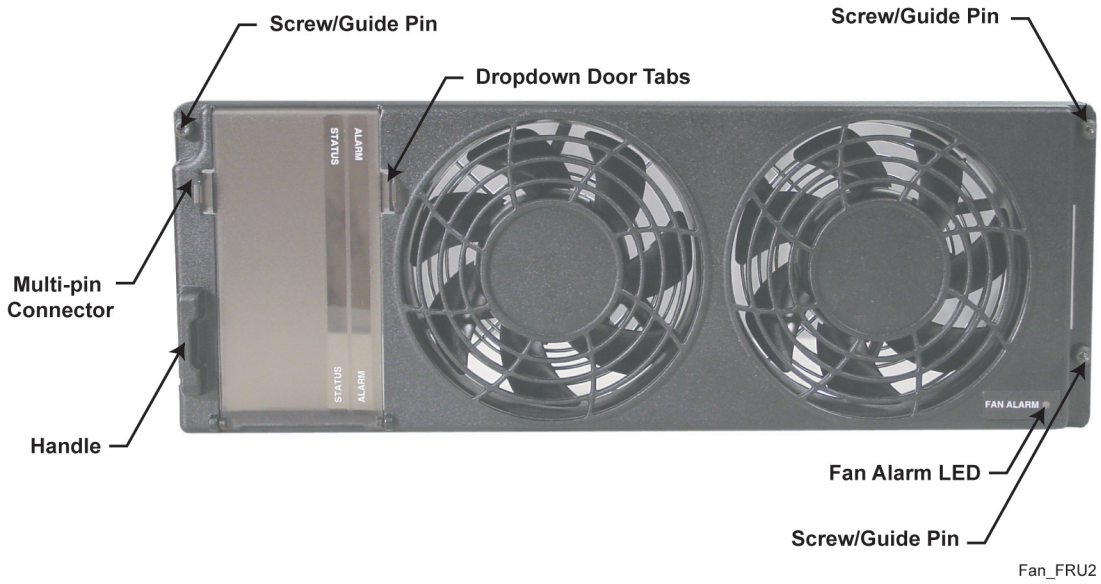
9.4 Replacing the Fan Assembly

WARNING: When removing a fan module, care should be taken to avoid contacting moving fan blades before and after removal with tools, hands, or other objects. If you are removing the fan module to access or replace the modules behind it, turn off the equipment power and allow the modules to cool before performing any work, as the surfaces of the modules can be extremely hot.

CAUTION: To prevent overheating, this fan must be in place at all times, except during servicing.

IMPORTANT: The fan assembly can be swapped out without shutting the power off. The replacement fan assembly must be in place within a reasonable amount of time so that the device module does not overheat and shut down.

Figure 28: Fan Assembly



When and where to use: Use this procedure to remove the fan module to replace the modules it covers.

Procedure:

1. Wear an Electrostatic Discharge (ESD) wrist strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout this procedure to prevent ESD damage to any components.

2. Using a T20 bit, loosen the three captive screws on the front of the fan assembly, so they disengage from the chassis.
3. Using the handle on one end and the edge on the other side, gently pull the fan assembly straight out to disengage the connector.
4. Using the guide pins and the connector on the back of the new fan assembly, push the new fan assembly into place until it feels secured.
5. Using a T20 Bit, tighten the three captive screws on the front of the fan assembly. Torque to 17 ± 2 in-lb.
6. Verify that the fan assembly is operating properly, and the Fan Alarm LED is off. Use software tools such as Unified Event Manager (UEM) or Configuration/Service Software (CSS) to verify the status of the equipment.

9.5 Replacing the Power Supply

IMPORTANT: The comparator power supply can be swapped out without shutting the power off, if the comparator is cabled to use the Auxiliary Power input from a colocated comparator. If the comparator is not cabled for this, the power must be shut off to replace the power supply.

Figure 29: Power Supply

Procedure:

1. Wear an Electrostatic Discharge (ESD) wrist strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout this procedure to prevent ESD damage to any components.

2. Push the power button to Off on the power supply unit.
3. Using a T20 bit, loosen the two captive screws.
4. Pull on the metal handle to disengage the power supply from the backplane, and remove it completely from the chassis.
5. Slide the replacement power supply into place, pushing gently until it seats.
6. Using a T20 bit, tighten the two captive screws.
7. Turn **On** the power button, and verify that the power supply is operating properly.
   - The power supply Status LED is green
   - The power supply Alarm LED is off
   - The power supply Fan LED is off
   - Use software tools, such as UEM, to check the alarms of the equipment.

9.6 Replacing the Backplane

When and where to use:
In a GCM 8000 Comparator, the “backplane” is the circuit board at the rear of the card cage, which connects the power supply and comparator modules. Use these procedures to replace the backplane.

NOTICE: The procedure assumes the following service access clearances:

- At least 2 ft access at the rear of the cabinet or rack, or
- At least 2 ft access on one side of the cabinet or rack, and at least 6 in. at the rear of the cabinet or rack.

Procedure:

1. Wear an Electrostatic Discharge (ESD) strap and connect its cable to a verified good ground. Be sure to wear this strap throughout this procedure to prevent ESD damage to any components.
2. If the comparator modules are not operational, go to step 7.
3. For a trunked comparator module, disable the comparator module as follows:
   a. Connect to the comparator module using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 78 in the Configuration chapter.

      NOTICE: If all unused ports on the LAN switch are disabled, enable the desired port. See the *System LAN Switches* manual.

   b. From the menu, select **Service** → **Status Panel Screen**.

      The **Status Panel Screens** window appears.

   c. Select the **Comparator** tab.

   d. In the **User Requested Comparator State** list box, select **User Disabled**.

   The comparator is disabled.
4. If another trunked module is located in the chassis, then disable the other module.
5. Disconnect the Ethernet cable from the service port on the comparator module.
6. Push the power rocker switch to Off (O) on the power supply unit.
7. Label and disconnect all cables from the comparator backplane.
8. Remove the power supply module from the chassis as follows:

   WARNING: Allow the power supply module to cool before performing the following step, which exposes surfaces of the module that can be extremely hot.

   a. Using a T20 bit, loosen the two captive screws on the front of the power supply, so that they disengage from the chassis.

   b. Pull on the metal handle to disengage the power supply module from the backplane, and remove it completely from the chassis.
9. Remove the fan assembly unit to gain access to the comparator modules. See Replacing the Fan Assembly on page 120.
10. Disengage the comparator modules from the backplane as follows:
    a. Using a T20 bit, loosen the two captive screws on the front of each module, so that they disengage from the chassis.

    b. Using their handles, gently pull the modules until they disengage from the backplane.
11. Remove the fan cable from the backplane, accessing it from the front of the chassis, with the backplane still secured to the chassis, as follows:
    a. Follow the fan cable with your hand from its connector at the front of the chassis to its connection to the backplane, through the card cage section from which you removed the power supply module.

    b. Remove the fan cable multi-pin connector from the backplane.

NOTICE: Squeeze the top and bottom of the connector and pull the connector straight out from the backplane.

12 Using a T20 bit, remove the seven screws that secure the metal backplane cover and the backplane circuit board to the rear of the comparator chassis.

13 Remove the metal backplane cover and the backplane circuit board.

14 Place the new backplane circuit board in the same location and orientation as the one that you removed.

15 Seat the seven screws into the backplane circuit board and backplane cover. Start all screws before fully securing them.

16 Using a T20 bit, secure the new backplane circuit board and the backplane cover to the rear of the comparator chassis with the seven screws. Torque to 18 +/- 2 in.-lb.

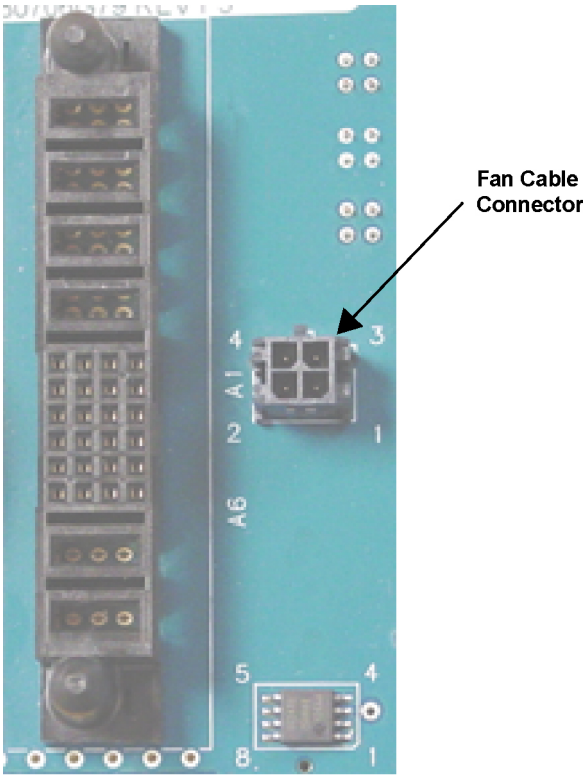
17 Connect the fan cable to the new backplane from the front of the chassis with the backplane secured to the chassis, as follows:

a Locate the port in the new backplane for the fan cable multi-pin connector.

b Follow the fan cable with your hand from its connector at the front of the chassis to the connector at the other end of the cable.

c Push the fan cable multi-pin connector, with the tab up, into the correct location in the backplane.

Figure 30: Fan Cable Connector



GTR_GCP_Fan_Cable_Connector

18 Slide the comparator modules into the new backplane. A slight push may be needed to engage the modules.

19 Secure the comparator modules to the chassis with the two captive screws on the front of each module.

20 Reinstall the fan assembly unit. See Replacing the Fan Assembly on page 120.

21 Slide the power supply into the chassis, pushing gently until it seats in the new backplane.

22 Tighten the two captive screws on the front of the power supply.

23 Reconnect all cables at the rear of the comparator.

24 Set the power supply rocker switch to On (1).

25 For a trunked comparator module, enable the comparator modules as follows:

a Connect to one of the comparator modules with the chassis, using Configuration/Service Software (CSS).

b From the menu, select **Service** → **Service Panel Screen**.

The **Service Panel Screens** window appears.

c Select the **Comparator** tab.

d In the **User Requested Comparator State** list box, select **Enabled**.

The comparator module is enabled after approximately two minutes.

e Repeat these steps for the other comparator module.

26 Disconnect the laptop PC from the comparator.

27 Verify that the LEDs indicate the modules you removed and reinstalled are operational:

- The Status LEDs are green
- The Alarm LEDs are off
- The power supply Fan LED is off

28 Verify proper operation using software tools, such as UEM, and CSS.

29 Re-configure the Security Settings into the backplane. See Setting the Serial Security Services in CSS on page 77.

This page intentionally left blank.

Chapter 10

GCM 8000 Comparator Disaster Recovery

This chapter provides references and information that will enable you to recover a GCM 8000 Comparator in the event of a failure.

10.1 Recovering the GCM 8000 Comparator

When and where to use:
Follow this process to recover the GCM 8000 Comparator field replaceable unit (FRU).

Process:

1. To replace, install, connect power, and cable the comparator, see GCM 8000 Comparator Hardware Installation on page 50.
2. To replace the GCM 8000 Comparator module within the chassis only, see Replacing the GCM 8000 Comparator Module on page 116 and perform steps 1 through 14.
3. To replace other hardware devices within the chassis, see GCM 8000 Comparator FRU/FRE Procedures on page 115.
4. To perform basic device configuration and SWDL download, see Replacing the GCM 8000 Comparator Module on page 116 and perform steps 15 through 29.

10.2 Performing a Site Download

Procedure:

1. Connect an Ethernet straight through cable between the Ethernet port on the computer and the Ethernet service port on the site controller or the appropriate LAN switch. The service computer/ laptop IP address must be set to an address on the subnet of the local site, which varies depending on the site and zone numbers. See Connecting Through an Ethernet Port Link on page 78.

   NOTICE: If 802.1x services are enabled on the site controller, an 802.1x login account to connect to the Ethernet port is needed. An 802.1x account is a centrally managed account. See Chapter 6, “802.1x Service Port Procedures for GCP 8000 Site Controller” in the *802.1x Service Ports on Switches* manual.

2. Open the Software Download Manager application.

   CAUTION: It is crucial that a site software download is performed at the site to ensure that all devices are on the same software version, VLAN, and active bank. Failure to perform this step results in the replacement comparator channel to have a mismatch in software versions. If a mismatch in software versions occurs, the comparator may go into a configuration mode of operation with a reason of ‘Invalid Software Version’. If this occurs, the comparator must be reset.

3. From the **Advanced Options** menu, select the transfer type.

4 Download and install the necessary software onto the site controllers and comparators as follows:

a From the menu, select **Action** and choose one of the following:

- **Use DNS Server:** This is the default option and is recommended for most cases.
- **Use Standard ASTRO IPs (non-Tsub):** Legacy option which relies upon a built-in IP Plan rather than the DNS Server. This option is not supported for Trunking Subsystems (Tsubs).
- **DNS Override:** Use when running the Software Download Manager from a server that is not joined to the ASTRO® 25 system domain. In order to use a DNS server in the ASTRO® 25 system domain, the **Override DNS Server** dialog box is used to specify the DNS server IP address (defaults to the ASTRO® 25 system level DNS server).
- **Load DNS File:** Use only in situations where a custom DNS configuration file has been provided. Typically, this option is selected when the site IP addresses are not configured to be part of an ASTRO® 25 system.

b From the menu, select **File** → **File Manager**.

The **Software Depot File Manager** opens.

c From the menu, select **Component Operations** → **Import Fileset**.

The **Import a Fileset Into the Software Depot** dialog box appears.

d Click **Browse** and search for the `swdlv3.cfg` file, or follow path: `E:\swdl\swdlv1.cfg` or `swdlv3.cfg`. Click **Open**.

The file appears in the **Configuration File Path** field of the dialog box.

e Click **Generate**. Click **OK**.

The **Import a Fileset Into the Software Depot** dialog box closes and the software component appears in the **Components In the Software Depot** list of the **Software Depot File Manager** window.

f Exit the **Software Depot File Manager**.

g From Software Download Manager, click **Open Site Mode**.

h From the **ASTRO 25 System Site Type** field, select the type of site.

i Select the **Zone**, **Site**, and if applicable, the **Subsite**. The Subsite ID is only available when the Site ID is between 1-64.

j Click **Connect**.

k If the device supports SNMPv3 protocol, a pop-up window appears with the security level option. Choose the required security level. Click **OK**.

NOTICE: Depending on the size of the system, the window takes a few minutes to update.
If the Ethernet connection to the site uses the Site Controller Service Port, you might need to enter an 802.1x login account to connect to the SC Service Port. An 802.1x account is a centrally managed account.

The system connects to the specified zone and site.

l If this is a simulcast site, from the **Site View** tab, click the icon in front of the **Prime LAN** folder, and **Subsite** folders.

The entries under the **Running Version** column display the current version. The **VLAN** column displays the VLANs for all devices.

m In the **Operation Type**, select **Transfer and Install**.

n For the **Application Type**, select **Comparator** and **Multisite Controller**.

o In the **Software Component** drop-down list, select the version for each site device.

NOTICE: Both device software must be chosen as part of the site software download.

p In the **Simultaneous Channels Install** drop down list, select the number of the channels to install simultaneously.

Software Download Manager always installs all channels. For example, setting the **Simultaneous Channels Install** field to a specific number value means that those amounts of channels are installed simultaneously.

NOTICE: The **Simultaneous Channels Install** field decreases the installation time. A warning is displayed if the site goes into failsoft, due to this setting.

q Click **Start Operation**.

NOTICE: If the **Start Operation** button is grayed out, SWDL has determined that there is a problem performing this operation to the selected devices. The button becomes active, when the appropriate operation set details are selected.
If a fileset is damaged, the Transfer operation stops. Import a correct fileset and repeater the operation.

r In the window that appears, click **Proceed**.

The Transfer operation begins first. After the transfer is successfully completed, SWDL begins the Install operation.

If the install was successful, the **Operation Status** bar displays green. If the install failed, the **Operation Status** bar displays red.

s Verify that the selected devices have installed the desired version of the software.

NOTICE: In most cases, the new software version is present in the **Running Version** column.
For more information, consult the “Fixing a Transfer Failure” section of the *Software Download Manager* manual.

In many cases, a second attempt at transferring the software corrects the failure. If further attempts continue to fail, contact System Support.

This page intentionally left blank.